UNIVERSIDAD TECNOLÓGICA DEL PERÚ

Facultad de Ingeniería

Carrera Profesional de Ingeniería de Sistemas e Informática

Programa Especial de Titulación

IMPLEMENTACIÓN DE LA METODOLOGÍA PMBOK Y MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE INDUCCIÓN DE PERSONAL EN LA EMPRESA JP LOGÍSTICA SAC

Alumno:

LÓPEZ LEIVA, YOEL WALTER

Para obtener el Título Profesional de
Ingeniero de Sistemas e Informática

Lima – Perú

2019

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

CAPÍTULO 1
ASPECTOS GENERALES

En este capítulo se da a conocer los problemas que se suscitan en la Empresa JP Logística S.A.C. con relación al análisis con gestiona miento en alarmas de seguridad en las informaciones, que propone el presente trabajo considerar los procedimientos para implementación de la metodología PMBOK Y MAGERI.T. siguiendo la terminología de la norma ISO 27002.

Específicamente en esta sección, se describirá el problema identificado, los objetivos, el alcance y el estado del arte del proyecto.

1.1. Definición del Problema

1.1.1. Descripción de la problemática

La Empresa JP Logística S.A.C. es una importante organización logística en expansión, encargada de brindar servicios integrales de transporte de carga de mercancías a nivel nacional, donde laboran aproximadamente 165 colaboradores, donde presenta limitaciones porque no tiene identificado los activos dentro del proceso de gestionamiento en alarmas que soportan los Sistemas de informaciones, a fin implementar las medidas apropiadas para controlar los alarmas y amenazas en la empresa.

En ese sentido, la empresa JP Logística S.A.C dispone de masivo almacenamiento de informaciones, y, por ende, se percibe que la seguridad

en las informaciones, están relacionados con los procesos, los alarmas informáticos físicos y lógicos, que están expuesto por su propia naturaleza, y por la interacción humana, ya que no existe una adecuada documentación de las actividades de alarmas, creando limitaciones al momento de gestionarlos, presentándose problemas e incidentes en muchos casos frecuentemente, y que son resueltos de manera reactiva y temporal, sin los fundamentos adecuados y estandarizados.

Por estas razones, se urge y se hace necesario realizar el análisis y gestionamiento en alarmas de la seguridad en las informaciones en el proceso de inducción del personal en la Empresa JPLogísticaS.A.C., con el fin de determinar los alarmas a los cuales está expuesto el mismo y establecer directrices para que en el futuro se puedan implementar mejores prácticas para disminuir o eliminar los alarmas y controlar la productividad y efectividad de los sistemas de informaciones implementados en la empresa.

Asimismo, se presenta y existe una serie de inconvenientes y limitaciones que se están dando en la Empresa JP Logística S.A.C., tales como:

- Limitada gestionamiento en alarmas.
- Poco gestion de accesos a los recursos informáticos de la empresa.
- Las directricess de cifrado son mínimas en cuanto a la seguridad en las informaciones clave del negocio.
- Mínima física y ambiental en toda la empresa.
- Existe poca seguridad en las telecomunicaciones.
- Se carece de la adquisición y mantenimiento de sistemas de informaciones.
- Inadecuada gestión de seguridad en las informaciones por ausentismo de sistemas para gestión.
- Cortos directrices para seguridad que no se cuenta con unas politizaciones para seguridad en las informaciones.
- Deficientes alarmas para amenazas y vulnerabilidades acerca los activos de informaciones.

- Poco expertise en seguridad en las informaciones debido a limitadas capacitaciones del personal de sistemas.
- Limitada inducción del personal sobre los procesos gestionamiento en alarmas de la seguridad en las informaciones.

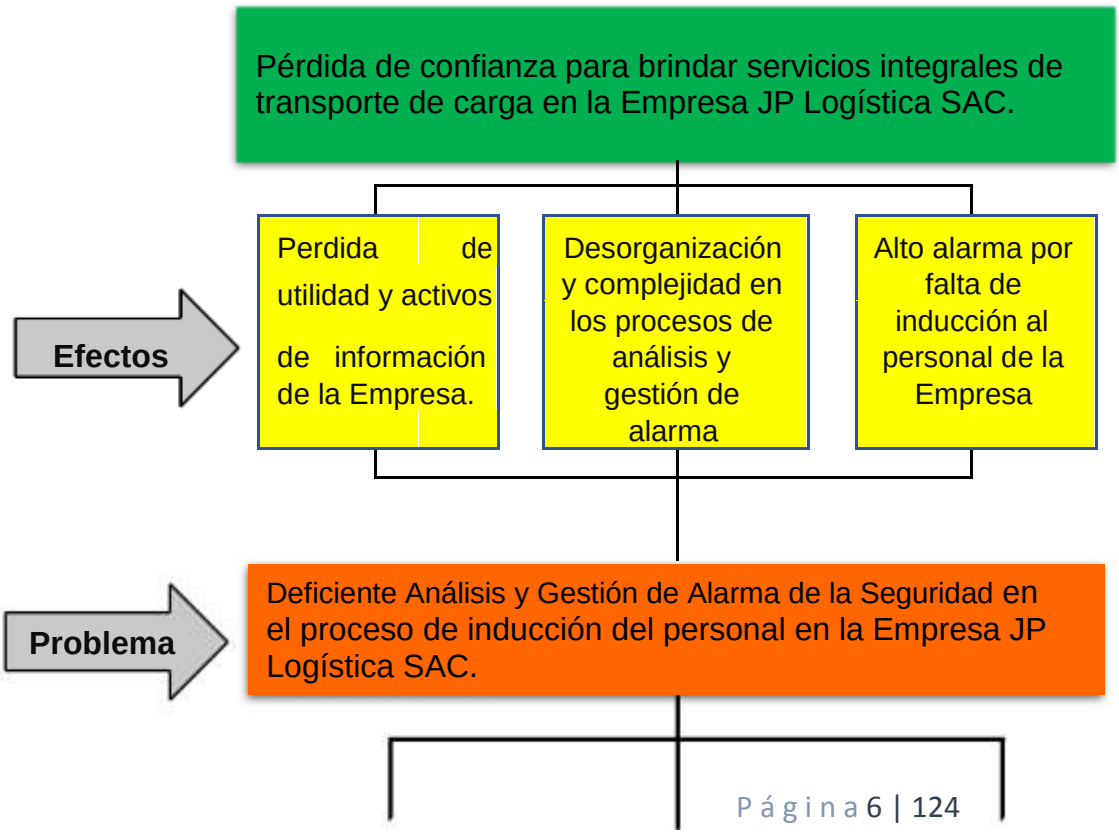
Limitaciones en la empresa, lo cual amerita el estudio responder la siguiente interrogante ¿Cómo proteger efectivamente la información y los procesos que la recolectan, procesan, almacenan y distribuyen, frente a los alarmas y amenazas de pérdida, divulgación, indisponibilidad o alteración en la Empresa JP Logística S.A.C.?

1.1.2. Formulación del problema de investigación

No existe implementado una metodología PMBOK Y MAGERI.T. para realizar el análisis y gestionamiento en alarmas de la seguridad en las informaciones de la Empresa JP Logística S.A.C.

1.1.3. Árbol del problema

Analizar y encontrar las causas, esto según Manual Práctico de Proyectos de Inversión (Conde, Núñez y Álvarez, 2008, p. 135).



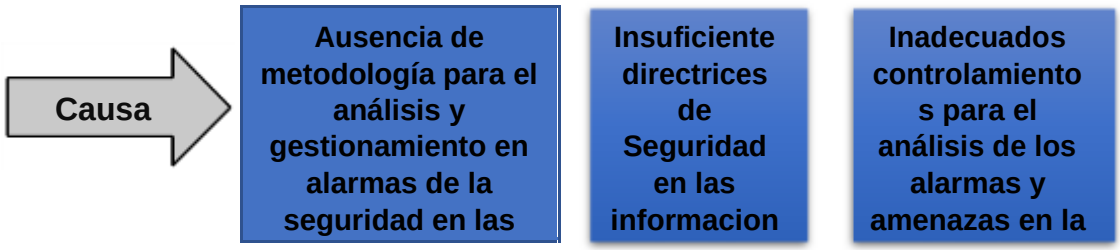


Figura 1. Árbol problemas

Fuente: Elaboración propia

Finalmente, en relación del problema central en el árbol del problema, se puede plantear el problema de investigación:

¿Cómo influye la implementación de la metodología PMBOK Y MAGERI.T. para el análisis y gestionamiento en alarmas de la seguridad en las informaciones en el proceso de inducción del personal en la Empresa JPLogísticaS.A.C.?

1.2. Definición objetivos

1.2.1. Objetivo general

Mejorar el análisis y la gestión en alarma de seguridad en las informaciones en el proceso de inducción del personal en la Empresa JPLogísticaS.A.C..

1.2.2. Objetivos específicos

- Inventariar y clasificar los activos del proceso de evaluación de personal y transportista en la Empresa JPLogísticaS.A.C..
- Analizar la gestionamiento en alarmas para el proceso Evaluación de Personal y Transportista en la Empresa JPLogísticaS.A.C..
- Establecer controlamientos para el mitigacionamiento de alarmas informáticos identificados en el proceso evaluación de personal y transportista en la Empresa JPLogísticaS.A.C..

1.3. Alcances y limitaciones

1.3.1. Alcances

1. El alcance se enfoca a la implementación de la metodología PMBOK Y MAGERI.T. para el análisis y gestionamiento en alarmas de la seguridad en las informaciones en el proceso de inducción del personal en la Empresa JPLogísticaS.A.C., el cual cubre los procesos más importantes, a fin de garantizar la operatividad, fiabilidad, seguridad para alcanzar el óptimo funcionamiento de los sistemas de informaciones, donde el personal debe conocer la situación real de la infraestructura tecnológica del Centro de Datos de la Empresa JPLOGÍSTICAS.A.C..
2. Se evaluará únicamente los procesos como históricos para la elaboración de documentos y operativos en la toma de decisiones para el mejor análisis de la gestionamiento en alarmas de los sistemas de informaciones en la organización.

1.3.2. Limitaciones

Las siguientes implicancias:

a) El tiempo que toma la implementación de la metodología PMBOK y MAGERI.T. aplicado a la inducción del personal de la empresa, es como máximo menor a medio año.
b) El análisis y gestionamiento en alarmas de la seguridad en las informaciones se encuentra únicamente enfocada al proceso de inducción del personal en la Empresa JPLogísticaS.A.C.,
c) La presente investigación precisa la norma ISO 31000, pero acepta y no discute otras normas para la implementación de sistemas de gestionamiento en alarmas de las empresas.

1.4. Justificación

El presente trabajo se justifica porque la data es tratada respecto a los activos mas críticos en las organizacionesas instituciones, provoca ventajas de competencia. (Najar & Suárez, 2015). Es decir, que la información reside en la informatica, sistemas para almacen, redes de data, agrupados en lo que se conoce como Sistemas de informaciones, los cuales se encuentran sujetos a alarmas y amenazas dentro y fuera de la organización.

Asimismo, se justifica porque la utilidad cual sea la forma, en que se toma en cuenta las amenazas y alarmas que acechan a las áreas que albergan la información y comunicación, es como jugar con la fortuna, se puede ser afortunado durante algún tiempo, pero tarde o temprano esa fortuna terminará, si no se toma las previsiones para la seguridad en las informaciones.

Finalmente, los beneficiaros de la investigación es la empresa, sus colaboradores y clientes, en vista, que se va disponer de mejores controlamientos para evaluación, análisis de la gestionamiento en alarmas para adoptar medidas relacionadas a sus causas, que es un elemento muy importante, por ende, será necesario implementar la metodología PMBOK y MAGERI.T. en el proceso de inducción del personal en la Empresa JPLogísticaS.A.C., definiendo el soporte como un manera crítico para éxito de la institución, emitiendo recomendaciones basadas en las mejores prácticas para evitar que estos se establezcan en la organización.

1.5. Estado del Arte

1.5.1. Casos internacionales:

Tema 1: Plan en gestionamiento en alarmas y gestión ética en el depto. de tecnología en ambito educativo.
Autor: Eduardo Ramón Bernal Alvear.
Lugar de investigación: Cuenca - Ecuador
Año de investigación: 2017

Resumen:

El mencionado Proyecto contemplóun trio típico de Depto.Tecnologías de informaciones Servicios Informátizados, Sistemas de informaciones y Red de Comunicaciones. Cuyo plan de gestionamiento en alarmas ISO/IEC/NTP 31000 para la gestionamiento en alarmas y los ISO 37001 ISO 26000 para la gestión ética. Dichos análisis de estas recomendaciones fueron elaborados con el artefacto PILAR, basado en la metodología MAGERI.T. y a través de encuestas a ingenieros de TI.

Análisis:

El mencionado proyecto es recomendado para todas las empresas de cualquier giro de negocio, en vista, que las plataformas en T.I. en empresas es constante incremento en respuesta a los clientes y servicios tecnológicos.

Como aporta a la presente investigación

Esta investigación aportó mediante la identificación de la importancia de la administración de plataformas en T.I., que es la más adecuada para la gestión en alarmas tecnológicos para vandalismo informático. Asimismo, se tomó el enfoque de análisis relevante de gestión como modelo para enfocarlo en la empresa JPLOGÍSTICAS.A.C..

Tema 2: Proyecto de Diseñamiento en las informaciones ISO 27002 para la alcaldía de Floridablanca y plan de acción para su implementación según la Guía Pmbok

Lugar de investigación: Colombia, en la alcaldía de Floridablanca de Bucaramanga

Año de investigación: 2014

Resumen:

El Proyecto de gestionamiento de seguridaden las informaciones a través de la norma ISO 27002, documentado en el contexto de los alarmas globales de cualquier organización, especificando la implementación de controlamientos de seguridad de acuerdo a las características de la organización, donde estos consideran la información como el activo más importante, por esta razón, se buscan medios para su protección debido a los grandes volúmenes de informaciones que maneja una empresa, los cuales están expuesta a alarmas.

Análisis:

El mencionado proyecto es recomendado para el Diseñamiento de sistematización de gestionamiento de seguridaden las informaciones ISO 27002, donde se verá reflejado en el crecimiento financiero de la entidad, de informaciones.

Como aporta a la presente investigación

Se tomó como base para la presente investigación el Diseñamiento e implantación de la sistematización de gestionamiento de seguridaden las informaciones, desde la perspectiva del acompañamiento de los controlamientos implementados para afrontar amenazas y vulnerabilidades.

1.5.2. Casos nacionales:

Tema 1: Sistematización de gestionamiento de seguridaden las informaciones y Alarmas de informaciones en seis sedes de entidad de finanzas de Perú

Lugar de investigación: Lima - Perú, Universidad Privada del Norte.
Año de investigación: 2018

Resumen:

El Proyecto se enfocó analizar y evaluar los levels en alarmas sucursales, cuya propuesta realizada fue la implementación del sistematización de gestionamiento de seguridaden las informaciones bajo la norma ISO/NTP/IEC 27001 y el modelo Deming, para ser aplicado por la misma entidad, permitiendo el cumplimiento de las normas de manera eficaz para la protección de los activos de informaciones de la sedes de los bancos.

Análisis:

El tema es recomendado e ideal para implementar sistematización de gestionamiento de seguridaden las informaciones en las áreas de Seguridad de informaciones, donde la Alta Gerencia debe tener en cuenta que analizar en la evaluación de los alarmas deben ser mitigados o terciarizar los servicios para establecer directricess de seguridad a través de las 6 sedes principales, que será de análisis y la evaluación de los alarmas que la entidad bancaria a nivel nacional.

Como aporta a la presente investigación

Se usó como punto de partida para la presente investigación, la preservación de los 3 puntos de seguridad enfocados inicialmente de la sede principal de la empresa JP Logística con la intención de evaluar la factibilidad propuesta para finalmente tomar

acciones sobre la implementación en los procesos de análisis y la evaluación de los alarmas.

Tema 2: Proyecto de Diseñamiento de un sistematización de gestionamiento de seguridadde informaciones para servicios postales del Perú S.A.

Autor: David Arturo Aguirre Mollehuanca

Lugar de investigación: Lima- Perú, Servicios Postales del Perú S.A.

Año de investigación: Pontifica Universidad Católica del Perú - 2014

Resumen:

El Proyecto evidencia IEC 27002 en las entidades públicas, que nace de la necesidad de gestionar adecuadamente la seguridad en las informaciones en cada una de estas empresas.Asimismo, se realizaron varias reuniones con la alta dirección de los servicios postales del Perú S.A que permitieron definir el alcance y las directricess del SGSI en la organización enfocándose en los procesos institucionales críticos de dicha entidad, a fin de identificar y valorar los activos críticos de la organización y evaluar los alarmas a los cuales estos estaban sometidos.

Análisis:

El mencionado proyecto es recomendado para el Diseñamiento de un sistematización de gestionamiento de seguridadde informaciones, debido a que es fundamental y necesario para que entendieran que el Sistematización de gestionamiento de seguridaden las informaciones, proteger información digital, sino la información crítica de negocio independizado de los dias.

Como aporta a la presente investigación

Se consideró el difundir las normas de seguridad en toda la empresa, poniendo como punto clave en la presente investigación, la difusión de una cultura de seguridad que antes no existía, donde estos no son conocidos ni reconocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.

Herramienta tecnológica basada en MAGERI.T.

El software EAR(Entorno de Análisis de alarmas) contiene los procesos de análisis y gestión del alarma de informaciones en la metodología MAGERI.T..

Frente a amenazas cuando ocurren, atentan los activos, generando impactos. Si evaluamos la continuidad con que se ejecutan las amenazas, podemos mitigar los alarmas al que se exponen al sistema. Reducción y continuidad que contabilizan las vulnerabilidades de los sistemas.

Los personales de los sistemas de informaciones cuentan contingencias, se reducen las frecuencias de ocurrencias, mitigan el impacto. Considerando el nivel de implementación de contingencias, el software pasa a una nueva estimación de alarma conocido como alarmas residuales.

PILAR cuenta con bibliotecas con estándares de propósitos generales, y realiza evaluaciones de seguridad usando normas conocidas como: ISO/IEC 27002 y Códigos de buenas prácticas para Gestionar la Seguridad de informaciones.

CAPÍTULO 2
MARCO TEÓRICO

2.1. Fundamento teórico

En particular este trabajo de investigación se focalizará en la implementación de la metodología PMBOK Y MAGERI.T. para el análisis y gestionamiento en alarmas de la seguridad en las informaciones en el proceso de inducción del personal en la empresa JPLogísticaS.A.C.. En tal razón, esto es fundamental considerar los procedimientos para identificar los alarmas en que podrían sufrir los activos de los Sistemas de informaciones frente a la amenaza que puede materializarse en la Empresa JP Logística S.A.C.

2.1.1. Antecedentes

La investigación profesional se ha podido viabilizar los siguientes antecedentes:

2.1.1.1. Antecedentes nacionales

Llontop, G. C. (2018). *Gestionamiento en alarmas de Tecnología de informaciones de las organizaciones de Nephila Networks.*. Universidad César Vallejo – Perú. Cuyo objetivo fue descripción de niveles de eficiencia en gestionamiento de alarma de tecnologías de informaciones de las empresas comerciales y de servicios de Nefila. Donde se evidencia, que muchas empresas brindan soporte a organizaciones que no desean invertir mucho en la dedicacion de sus gestores de sistemas, dedicándose más al implementar de su core de negocio, dando paso a los especializados en gestión y soporte de Tecnologías de informaciones (TI), Nefila que brinda y asegura un alto nivel de soporte; donde cada empresa gestionaba sus alarmas según su experiencia, es así que; Nefila implementó en un modelo de gestionamiento en alarmas general. Aplicación de métodos de estadística los resultados fueron, que la eficiencia con la que se gestiona los alarmas en cada tipo de empresa difiere en cuanto a la eficiencia y se plantean algunas mejoras para la incrementación de la eficiencia del modelamiento utilizando

en este tipo de organizaciones, y así la mejora del gestionamiento en alarmas.

García, S. C. (2018). *Modelamientos de seguridad en las informaciones para anadir unidades de ambientes de región Lambayeque*. Universidad Católica Santo Toribio de Mogrovejo, Chiclayo – Perú. Cuyo objetivo fue contribuir en la seguridad en las informaciones de la gestión de las unidades ambientales de la región Lambayeque, en las informaciones basado en metodologías y marcos de trabajo adaptados a la gestión de las unidades de ambiente. El modelamiento validado se aplicó a 1 caso de estudio para 1 unidad ambiental de Lambayeque, con 21 alarmas que fueron alineados con 23 controlamientos propuestos, monitoreando 23 controlamientos igual a la seguridad en las informaciones logra contribuir a la gestión de unidades.

Cruz, M. A. y Fukusaki, S. (2017). *Diseñamiento e implemenación de un sistematización de gestionamiento de seguridad en las informaciones para proteger los activos de informaciones de la Clínica MED-CAM Perú SA.*. Universidad de San Martín de Porres, Lima – Perú. Objetivos diseñar e implementar un Sistematización de gestionamiento de seguridad en las informaciones con el fin de cuidars activos de informaciones que influyan en el cumplimiento de objetivos organizacionales. Se logró implementar un SGSI con lo que se minimizó alarmas de informaciones de MEDICAM Perú S.A.C. y así, lograr la disponibilidad e integridad en las informaciones.

2.1.1.2. Antecedentes internacionales

Poma, E. F. (2017). M*etodología para el gestionamiento en alarmas.* (Tesis para optar el grado académico de Magíster en Gestión Estratégica de Tecnologías de la Información). Universidad de Cuenca, Cuenca - Ecuador. Tuvo como objetivo fue desarrollar una Guía Metodológica para la Gestionamiento en alarmas en una empresa PyME del

privado, basada en la norma ISO 31000:2011. Luego del análisis realizado en la empresa se concluye que el nivel de conocimiento de la gestión de alarma en la empresa, no tiene bien definidos los procesos en la gestión de compras, y tampoco los procesos para la correcta gestión de la alarma, lo cual este permitirá la identificación, manejo y control, para reducir la incertidumbre en todas las actividades relacionadas con los procesos y la toma de decisiones. Es importante que los directores y mandos medios apliquen la implementación de la *Norma ISO 31000:2011*, a fin de incrementar la probabilidad de éxito, de alarmas, desarrollado matrices en cada uno de los elementos del marco de la gestión de alarma, para generar la cultura de mejora continua en los procesos de gestión de alarma, lo que permitirá que los objetivos y metas de la empresa se vean cumplido, a través de los criterios de alarma para el establecimiento de directrices de alarma.

Yáñez, N. A. (2017). *Sistematización de gestionamiento de seguridaden las informaciones para la subsecretaria de economía y empresas de menor tamaño*. (Tesis para optar el Grado Académico de Magíster en Tecnologías de informaciones). Universidad de Chile, Santiago de Chile. Tuvo como objetivo en la ISO27002:2013, bajo una estrategia de mejora continua de procesos en una institución pública. Directricess y procedimientos de seguridad en las informaciones se realizaron dos auditorías, una interna y otra realizada por una empresa externa. Ambas auditorias llegaron a la conclusión que el estado actual de seguridad en las informaciones estuvo en un nivel medio. Finalmente, las directricess y procedimientos de seguridad en las informaciones, continuar con la implementación de los restantes 70 objetivos de control de la norma ISO27002:2013 de las directricess y procedimientos de seguridad en las informaciones.

Gordillo, A. C. (2017). *Sistematización de gestionamiento de seguridaden las informaciones para EMEL-NORTE*. Universidad Técnica del Norte, Ibarra - Ecuador. Tuvo como objetivo en las informaciones para la Empresa Eléctrica Regional Norte mediante la aplicación de la norma ISO 27002 para brindar un soporte en la toma de decisiones gerenciales. Los

resultados de este análisis mostraban que un buen porcentaje de las utilidades en informaciones, para los cuales se han seleccionado una lista de controlamientos de la norma ISO NTP 27002 a ser aplicados a fin de minimizar dichas alarmas. Las fechas en las que la empresa deberá implementar estos controlamientos. Finalmente, para calcular las alarmas y su tolerancia. Permite llevar un registro de los controlamientos escogidos de la norma para mantener un control de desarrollo.

2.1.2. Marco teórico

Con el que se contextualizará las teorías básicas que usaran en el desarrollo de proyectos, nos muestra el interés de metodología Pmbok, MAGERI.T. para el análisis de la gestionamiento en alarmas y amenazas a los sistemas de informaciones, la Gestión Integral de Alarmas (ERM) que forma parte de las buenas prácticas de gestión empresarial, la seguridad en las informaciones en fundamento de la Norma ISO/IEC/NTP27005, con la Norma ISO 31000 para analizar el valor de la gestionamiento en alarmas en las organizaciones, la Norma ISO 27002 que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información y finalmente con la Norma ISO 27002 que es una guía de buenas prácticas que describe los objetivos de control y controlamientos en las informaciones.

2.1.2.1. Metodología del enfoque del PMI(PMBOK)

PMI (2013) es la guía de fundamentos para los proyectos conocido como Guía PMBOK acerca de proyectos; es la utilización conceptual de proyectos de manera que cumpla con metas. Se logra aplicar e integrar adecuadas a 47 procesos en dirección de proyectos, agrupados lógicamente, en 5 Grupos de Procesos y son: inicio, planificación, ejecución, trazabilidad y control y cierre (p. 5).

Por otra parte, Romero y Diez (2013) señala que guía de fundamentos para dirección (PMBOK); es comun divulgado a nivel de toda América. En países del tipo Colombia los métodos están siendo aplicados en el sector público y también en el sector privado, así como su garantía que es avalada por instituciones educativas (p. 158).

La metodología de la Guía del PMBOK sobre la dirección de proyectos, establece las fases siguientes:

1. Fases inicio:

   "Son aquellos procesos para hacer un nuevo proyecto existente al obtener la autorización para iniciar un proyecto o fase" (PMI, 2013, p. 49).

   Según Wong (2010) la fase inicial en esta fase se definió el alcance de proyectos y el desarrollo de casos de negocio. Se identifican todas las entidades con los actores y se define alto nivel de abstracción: Identificar los casos de uso, describirlos en detalle (p. 51).

2. Fase planificación:

   "Son requeridos para el alcance de proyectos, refinar objetivos y definir acciones para alcanzar objetivos por proyecto" (PMI, 2013, p. 49).

   Para Craig (2003) manifiesta granularizada de los proyectos, el desarrollo iterativo del núcleo de la arquitectura, analizando las alarmas altas, requisitos, donde las estimaciones reales" (p. 19).

3. Fase ejecución:

   "Para que los requisitos del mismo" (PMI, 2013,p.49).

   Según Wong (2010) la fase para construir; "se construye el producto, desarrollando a detalle el Diseñamiento y produciendo el código. En esta fase todas las componentes restantes se desarrollan e incorporan al producto" (p. 51).

4. Fase monitoreo y control:

   "Procesos utilizados para rastrear y regular progresos y desempeños de los proyectos, para dar áreas en el plan requiera los cambios para comenzar" (PMI, 2013, p. 49).

   Para Craig (2003) indica las fases y los despliegues".

5. Fase cierre:

"Procesos requeridos para culminar, a fin de finiquitar proyectos" (PMI, 2013,p.49).

Según Wong (2010) indica que fases de cierre; "se implementan productos a la comunidad de los usuarios. Instalado nacerán elementos que significarán desarrollos y/o ciclos" (p. 52).

En resumen, la fase de culminadas para la utilización de los usuarios finales.

Por otra parte, el PMI (2013) afirma que la "gestión de alarma", es un evento, que, de producirse, tiene efectos positivos o negativos. Una alarma puede tener una causa de materializarse, un impacto.

En ese contexto, la definición dada por el PMI, nos da luz sobre el concepto de la alarma, identificar y minimizar el impacto, una tarea relevante para los objetivos requeridos, conociendo el medio en que se aprecia para poder evitar las consecuencias y efectos sobre los negativos dentro de la organización.

Para Sommerville (2011) en gestión de la alarma. Se deriva de requisitos vagamente definidos, cambios de requerimientos que hacen cambios en necesidades de clientes.

En definitiva, Sommerville pone énfasis en las distintas actividades negativas de usuarios, cliente, herramienta, que dificultan el correcto desarrollo de los eventos, por ende, pone cuidado en analizar estos requisitos para los posibles efectos negativos en la empresa.

2.1.2.2. Metodología MAGERI.T.

MAGERI.T. es el acrónimo de "Metodología de Análisis y Gestionamiento en riesgos de los Sistemas de informaciones.

"La Metodología de Análisis y Gestionamiento en alarmas de sistemas de informaciones de las Administraciones públicas, MAGERI.T., las alarmas

que soportan los Sistemas de informaciones, y para las medidas que deberían controlar estas alarmas." (Paredes, 2011, p. 109).

Asimismo, en MAGERI.T. versión 3 persigue los siguientes objetivos: Directos:

- Concienciar a los responsables de las organizaciones de informaciones de la existencia de alarmas y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los alarmas derivados del uso de plataformas en T.I.y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los alarmas bajo control.

Proceso de la metodología MAGERI.T.

Las actividades que se realizan en la metodología MAGERI.T. cumplen con un proceso que tendrán un lineamiento para llegar a los resultados propuestos que será explicado a continuación:

1. Activos: Se refiere los activos que posee la Organización categorizados de acuerdo a su función.
2. Valoración Activos: Es la valoración establecida al activo de acuerdo a la criticidad.
3. Identificación de Amenazas: Son eventos que reducirían el valor de los activos.
4. Frecuencia: Se refiere a los eventos que se producen en un tiempo determinado.
5. Degradación: Es que tan perjudicado quedaría el activo al materializarse las amenazas.
6. Alarma: Es la probabilidad de materialización de amenazas sobre el activo.
7. Identificación y Valoración de Salvaguardas: Son las acciones concretas para reducir el alarma;

8. Alarma Residual: Es el alarma remanente después de emplear las salvaguardas.

Figura 2: Proceso MAGERI.T.

Fuente: (Ramos, 2012)

Método de Análisis de Alarmas

El análisis de alarmas es una aproximación metódica para determinar el alarma siguiendo unos pasos pautados:

- Determinar activos importantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio supondría ..
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al alarma.
- Estimar el alarma, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Finalmente, para un correcto de Gestionamiento en alarmas se deberá ejecutar dos grandes tareas:

- Análisis de alarmas, que permite determinar qué tiene la Organización y estimar lo que podría pasar.

- Mitigacionamiento de alarmas, que permite la defensa concienzuda, defendiendo para que no pase algo malo y al tiempo estando preparados para atajar las emergencias, y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el alarma se reduce a un nivel residual que la Dirección asume.

2.1.2.3. Gestión Integral de Alarmas (ERM)

La conceptualización de gestión integral de alarmas, o también denominada administración de alarmas, los alarmas que puedan afectar el cumplimiento de sus objetivos. Esto con el fin de emprender en forma efectiva las medidas necesarias para responder ante ellos. (Mejía, 2006, p.41).

En ese contexto, existe estándares que se aplican en la Gestión Integral de Alarmas de gestionamiento en alarmas, donde recoge toda la visión de las alarmas y da una metodología integradora.

2.1.2.4. Norma ISO/IEC 27005

La norma ISO/IEC 27005:2008, provee lineamientos para la gestionamiento en alarmas de seguridad en las informaciones en una organización, dando soporte en particular a los requerimientos de un Sistematización de gestionamiento de seguridaden las informaciones (SGSI) de acuerdo a la norma ISO/IEC 27002.

Para la norma ISO/IEC 27005, el proceso de gestionamiento en seguridad en las informaciones, consiste en los puntos señalados en la figura 2:

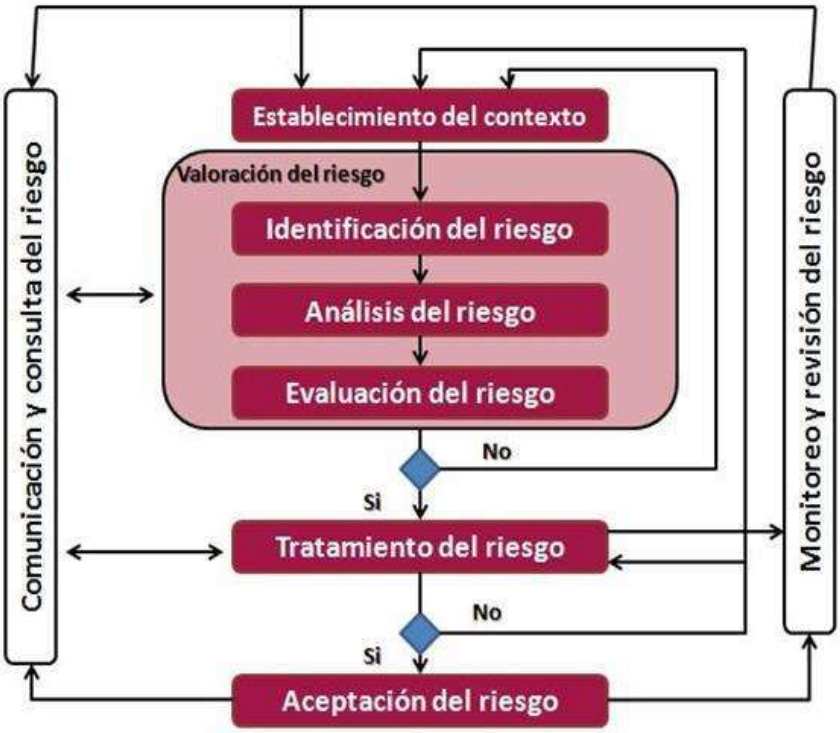


Figura 3: Proceso de gestionamiento en alarmas de seguridad en las informaciones

Fuente: Norma ISO 27005:2008

En la figura anterior, se puede ver como el proceso de gestionamiento en alarmas de la seguridad en las informaciones comienza con establecer el contexto, y luego con la valoración de alarmas, que incluye la identificación, estimación y evaluación de la alarma.

Luego hay un punto de decisión donde se mide si hay suficiente información las acciones requeridas para modificar las alarmas a un nivel aceptable para entonces llenar y tratar; si no hay información suficiente se debe realizar otra iteración, regresando al establecimiento del contexto. Cuando el tratamiento de la alarma no ha sido efectivo, no se obtiene un nivel de alarma residual aceptable, entonces será necesaria otra iteración hacia el contexto.

Finalmente, las aprobaciones de alarmas deben ser explícita en la alta directiva de la organización. Durante el proceso de la gestionamiento en alarmas de seguridad en las informaciones, es necesario que los alarmas y su tratamiento sean comunicados al alta directiva y al personal operacional exitoso.

2.1.2.5. Norma ISO 31000

El gestionamiento en alarmas, que puede ser utilizado por cualquier organización de acuerdo a su tamaño.

A través del "uso de ISO 31000 ayuda a organizaciones a crecer la probabilidad de alarmas". (ISO, 2011). Sin embargo, la ISO NTP 31000 comparar prácticas de gestionamiento en alarmas con un reconocimiento nacional o internacional.

Asimismo, las alarmas, por lo que se centrara el estudio del alarma tecnológico específicamente en un Departamento de Tecnología. Cuando la gestión del alarma, dicha gestión le permite a la organización, tener los siguientes beneficios:

Tabla 1.

Beneficios de la norma ISO 31000

Aumentar probabilidades de alcanzar metas.
Promocionar gestión proactiva.
Ser consciente e identificar y tratar alarmas en toda la organización.
Mejorar la presentación de informes obligatorios y voluntarios.
Mejorar los controlamientos.
Asignar eficazmente los recursos para el tratamiento del alarma.
Mejorar la eficacia y la eficiencia operativa.
Mejorar la prevención y la gestión de incidentes.
Minimizar las pérdidas.
Mejorar aprendizaje organizacional.
Mejorar flexibilidad organizacional

Fuente: (NTE-INEN-ISO 31000, 2014)

Se trata de un estándar que puede aplicarse a cualquier tipo de organización, más allá de su naturaleza, actividad, escenario comercial o tipo de producto, entre otros factores. Alarma para reducir los obstáculos que impiden la consecución de sus objetivos, siendo compatible con cada sector**.** (Norma ISO 31000, 2011, p. 4).

La norma ISO 31000 define la Gestionamiento en alarmas como todas aquellas acciones coordinadas para dirigir y controlar los alarmas. La gestión tiene que ver, sobre todo, con la cuantificación de alarmas, para lo cual es fundamental definir dos elementos dentro de este proceso:

- Consecuencia: En este caso, se trata de evaluar los alarmas que cumplen con la premisa de causa-efecto.

- Probabilidad: Este segundo término habla de la posibilidad de que un hecho se produzca. Para la Gestionamiento en alarmas.

Metodologías de análisis de alarmas

Dado que los alarmas no tienen el mismo origen ni la misma naturaleza, existen varias estrategias para su gestión. Análisis de alarmas se dividen en dos grupos principales:

a) Metodologías de gestión del alarma:

Son aquellas que están orientadas a la identificación, evaluación y el posterior mitigacionamiento de alarmas derivados de una actividad. Entre ellas está, como es obvio, la norma ISO 31000.

b) Metodologías de cuantificación:

En este caso, se trata de aquellas herramientas que exclusivamente en la cuantificación de las alarmas.

- MAGERI.T.: se trata de una metodología de análisis y gestionamiento en alarmas que ha sido elaborada por el Consejo Superior de Administración.
- Delphi: es un método orientado a conocer la opinión de expertos.

Proceso de gestionamiento en alarmas

La norma ISO 31000 tienen enfoques. La implementación de un Sistema de Gestionamiento en alarmas, para ser eficaz y cumpla con objetivos trazados al inicio.

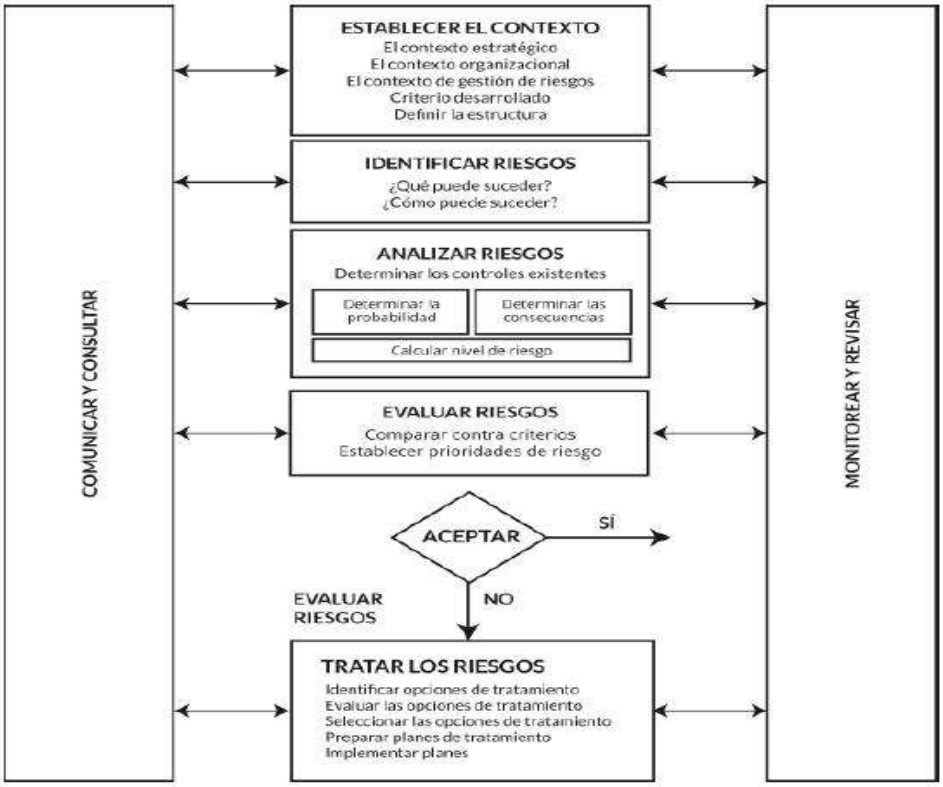


Figura 4. Procesos de gestionamiento en alarmas

Fuente: Norma ISO 31000 (2011, p. 14)

2.1.2.6. Norma ISO 27002

ISO 27002 es una norma internacional emitida que describe cómo gestionar la seguridad en las informaciones en una empresa (Kosutic, 2013). Esta norma brinda modelos de creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistematización de gestionamiento de seguridad en las informaciones (SGSI) adoptando un enfoque por proceso, basado en el Ciclo de Deming.

Las alarmas potenciales que pueden afectar la información, mediante una evaluación de alarmas, para posteriormente definir las acciones necesarias para reducir dichas alarmas, lo cual se conoce como mitigación de la alarma.

Esta norma fue publicada en octubre de 2005; en ella se especifican los requerimientos en establecer, implementar, mantener y mejorar la sistematización de gestionamiento de seguridad en las informaciones, y mitigacionamiento de alarmas de seguridad en las informaciones.

A continuación, la figura 5 muestra la reorganización de las cláusulas principales de la versión 2005 a la publicada en 2013.

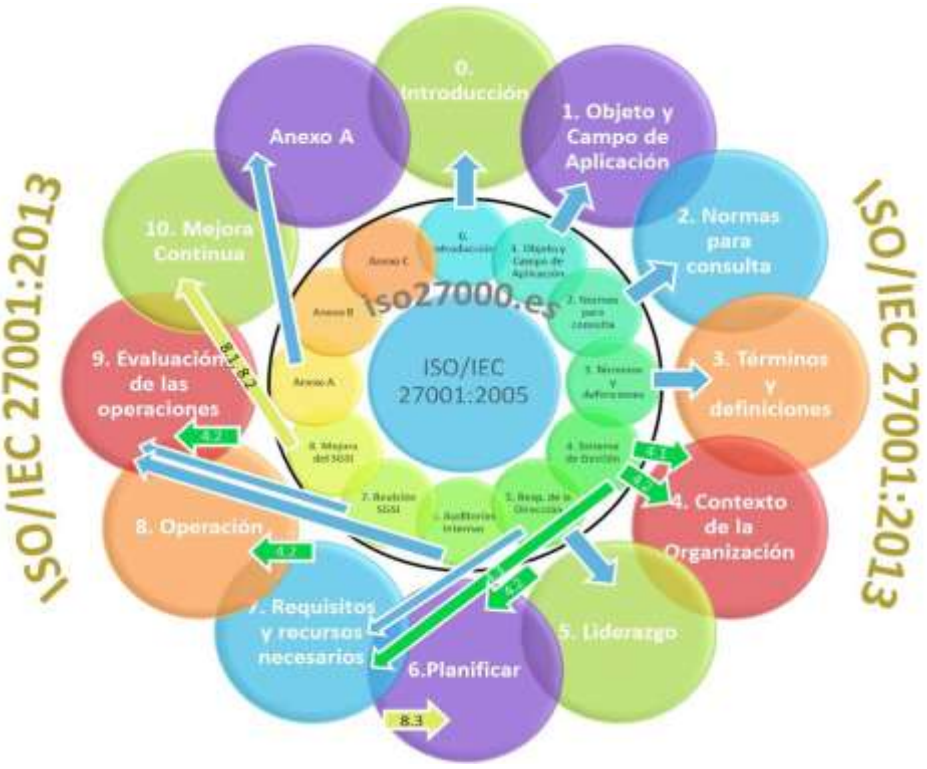


Figura 5. Comparación de la ISO/NTP/IEC 27001:2005 e ISO/IEC 27002:2013

Fuente: Adaptada del portal de ISO 27002 en español.

Cláusula 1 – Ámbito

Incluye requisitos para valorar y tratar alarmas de la seguridad en las informaciones.

Cláusula 2 - Referencias normativas

Se hace una referencia normativa en parte, o en su totalidad, norma ISO/IEC 27000, Information Technology. Security Technology Techniques.

Cláusula 3 - Contexto de las organizaciones

Se determina externos e internos de la organización, las necesidades de partes interesadas y el alcance de todo el SGSI.

Cláusula 4 - Términos y definiciones

Se aplican términos y definiciones proporcionados en ISO/IEC/NTP 27000.

Cláusula 5 - Planificación

Las alarmas y oportunidades para tratarlas, se valora cada alarma identificada de alarmas de seguridad en las informaciones. La organización en las informaciones a niveles y funciones relevantes.

Cláusula 6 - Liderazgo

Se establece unas politizaciones para seguridad de informaciones.

Cláusula 7 - Soporte

Mejorar continuamente de la sistematización de gestionamiento de seguridad en las informaciones.

Cláusula 8 - Evaluación del desempeño

Las sistematizaciones de gestionamiento de seguridad en las informaciones.

Cláusula 9 - Operación

En las informaciones. Se realiza la evaluación de alarmas de seguridad en las informaciones.

Cláusula 10 - Mejoras

La organización debe mejorar la conveniencia, y efectividad de la sistematización de gestionamiento de seguridad en las informaciones.

Dentro del análisis, directrices. ISO 27002 ha detallado cómo amalgamar todos estos elementos dentro del sistematización de gestionamiento de seguridaden las informaciones (SGSI).

Finalmente, en las informaciones no se acota solamente a la seguridad de TI, por ende, la filosofía principal de la norma ISO 27002 se basa en la gestionamiento en alarmas: investigar dónde están los alarmas y luego tratarlos sistemáticamente (Instituto Nacional de Tecnologías de la Comunicación, 2017).

Norma Técnica Peruana "NTP ISO/IEC 27002:2014

Donde se aprueba el uso de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad en las informaciones. Requisitos. 2a. Edición".

Es importante destacar, que esta NTP de seguridad en las informaciones tiene como Sistematización de gestionamiento de seguridaden las informaciones ISMS, por sus siglas en inglés (Information Security Management System).

En términos generales, la Norma Técnica Peruana cubre todo el tipo de organizaciones dentro del contexto de los alarmas de negocio de la organización. Especifica los requisitos para implementar los controlamientos de seguridad adaptada a las necesidades individuales de las organizaciones o partes de la misma tiene como modelo.

Finalmente, información de los interesados en las informaciones (es decir: gestión de la seguridad en las informaciones).

2.1.2.7. Norma ISO 27002

La norma ISO/IEC/NTP 27002, es recopilación de las mejores prácticas para Gestionar Seguridad en las informaciones.

En cuanto a seguridad en las informaciones la ISO 27002:2013, contiene 39 objetivos de control y 114 controlamientos, agrupados en 14 dominios de seguridad. Esta norma se encuentra publicada en español a través de la empresa AENOR .

Tabla 2.

Dominios – Objetivos de Control y Controlamientos ISO 27002:2013

DOMINIOS (11)	OBJETIVOS DE CONTROL (39)	CONTROLES (114)
1. Políticas de seguridad.	Política de seguridad de la información	2
2. Aspectos organizativos de la seguridad de la información	2.1. Organización interna.	5
	2.2. Dispositivos para movilidad y teletrabajo.	2
3. Seguridad ligada a los recursos humanos	3.1. Antes de la contratación.	2
	3.2. Durante la contratación.	3
	3.3. Cese o cambio de puesto de trabajo.	1
4. Gestión de activos.	4.1. Responsabilidad sobre los activos.	4
	4.2. Clasificación de la información.	3
	4.3. Manejo de los soportes de almacenamiento.	3
5. Control de acceso.	5.1. Requisitos de negocio para el control de acceso	2
	5.2. Gestión de acceso de usuario.	6
	5.3. Responsabilidad del usuario.	1
	5.4. Control de acceso a sistemas y aplicaciones.	5
6. Cifrado.	6.1. Controles criptográficos.	2
7. La seguridad física y ambiental.	7.1. Áreas seguras	6
	7.2. Seguridad de los equipos.	9
8. Seguridad en la operativa.	8.1. Responsabilidades y procedimientos de operación	4
	8.2. Protección contra código malicioso.	1

	8.3. Copia de seguridad. 8.4. Registro de actividad y supervisión. 8.5. Control del software en explotación. 8.6. Gestión de vulnerabilidades técnicas. 8.7. Consideraciones de auditorías de los sistemas de información	1 4 1 2 1
9. Seguridad en las telecomunicaciones.	9.1. Gestión de la seguridad en las redes. 9.2. Intercambio de información con partes externas.	3 4
10. Adquisición, desarrollo y mantenimiento de los sistemas de información	10.1. Requisitos de seguridad de los sistemas de información. 10.2. Seguridad de los procesos de desarrollo y soporte. 10.3. Datos de prueba	3 9 1
11. Relaciones con suministradores.	11.1. Seguridad de la información en las relaciones con suministradores. 11.2. Gestión de la prestación de servicios por suministradores.	3 2
12. Gestión de incidentes en la seguridad de la información	12.1. Gestión de incidentes de seguridad de la información y mejoras.	7
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	13.1. Continuidad de seguridad de la información. 13.2. Redundancias.	3 1
14. Cumplimiento	14.1. Cumplimiento de los requisitos legales y contractuales. 14.2. Revisiones de la seguridad de la información.	5 3

La muestra de la Tabla 2, se establece donde se pueden lograr aplicando apropiadas estrategias de control, siendo los estándares ya elaborados una el inicio de este proyecto, pero cabe recalcar que cada organización maneja directricess, y recursos humano diferentes.

2.1.2.8. Seguridad en las informaciones

La seguridad en las informaciones y comunicaciones que dan soporte al negocio (Institución Nacional de Tecnologías de la Comunicación, 2017).

Por otra parte, Soriano (2014) define la seguridad en las informaciones como resguardar información y sistemas de informaciones de accesos, uso, divulgaciones, alteraciones, modificaciones, inspección, lectura, registro y/o destrucciones no autorizadas. La seguridad en las informaciones.

2.1.2.9. Importancia de la seguridad en las informaciones

La información y los procesos que apoyan los sistemas y redes son importantes activos de la organización. Por lo tanto, definir, realizar, mantener y mejorar la seguridad de informaciones.

Asimismo, las organizaciones de informaciones se enfrentan cada vez más, con alarmas e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática. Daños por ataques de informaciones o de negación se están volviendo cada vez más comunes, ambiciosos y sofisticados

Por lo tanto, "…la seguridad es un proceso multidimensional, y procesamiento de negocios." (Areitio, 2008).

Asimismo, Soriano (2014) señala que fundamentales de la seguridad en las informaciones han sido la *confidencialidad, integridad y disponibilidad. Luego* se fueron añadiendo; la autenticación, control acceso, no repudio y la privacidad. (p. 31).

2.1.2.10. Sistematización de gestionamiento de seguridaden las informaciones SGSI

SGSI o ISMS "*es las informaciones, integridad de la información mientras minimiza los alarmas de seguridad en las informaciones*". (Aguirre 2014:29).

Por otra parte, el Instituto Nacional de Tecnologías de la Comunicación, (2017) señala que un Sistema de Gestión en Seguridad en las informaciones, es una herramienta basada en ISO/NTP 27002 alarmas que atenten la seguridad en las informaciones dentro de una empresa.

De este modo, el propósito del SGSI, "*alarmas de la seguridad en las informaciones sean gestionados y minimizados por la organización estructurada, adaptada a cambios que se produzcan en los alarmas, el entorno y las tecnologías*." (ISO 27002).

Es decir, cuida a las organizaciones alarmas (Espinoza, 2015).

Consigue mantener el alarma. La ISO 27002, define que "*la seguridad en las informaciones consiste en cuidar la confidencialidad disponibilidad, integridad y de la información, así como de los sistemas implicados en su tratamiento de las organizaciones*".

Esto indica, que la gestión de los alarmas a través de un Sistematización de gestionamiento de seguridad en las informaciones permite preservar en el interior de la empresa, lo siguiente:

a) Confidencialidades

   Nadie debe poder leer los datos excepto las entidades específicas (Soriano, 2014, p. 32). La confidencialidad es un requisito:

   - Cuando almacenan los datos en un medio (tal como un disco duro de ordenador) al que puede acceder a personas no autorizadas.
   - Cuando datos se copian en un dispositivo que puede acabar en manos de personas no autorizadas.

b) Integridad

   Es el cuidado de data en la modificación, duplicación o reordenación realizada por entidades no. La integridad son los recursos de

informaciones. Una violación a la integridad es un ataque activo. (Soriano, 2014, p. 33)

Esto apoya, que la integridad es garantía de no alteración ni descubrimiento de alteraciones de data, es esencial en entornos empresariales electrónicos, y es deseable en otros entornos.

c) Disponibilidad

Acceso a información cuando se quiere. Una falla de disco en cualquier atraso superior al establecido en los niveles de servicio puede ser descrito como una violación de la disponibilidad. Si un sistema de informaciones no dispone dicho sistema. (Soriano,2014, p.34)

Asimismo, de la misma manera otros aspectos de seguridad, pueden verse cuestionsdos puramente técnicas , fenómenos naturales, o causas humanas.

Finalmente, la meta de seguridad información, es programar y gestionar programas de seguridad en las informaciones que alcance 5 resultados identificados , los cuales son:

1) Alineación tactica de seguridad en las informaciones.
2) Gestión efectiva de alarma mediante ejecución de acciones apropiadas para reducir alarmas e impactos en recursos de informaciones a un nivel aceptable.
3) Entrega de optimizaciones en informaciones en apoyo de los objetivos de organización.
4) Gestión de recursos con infraestructura de seguridad en las informaciones eficientes y efectivas.
5) Medición del desempeño en gobierno de seguridad en las informaciones para garantizar el alcance de metas de la organización.

2.1.3. Marco conceptual

Activos de informaciones

Son recursos que poseen valor o utilidad para la organización, donde la organización funcione y logre los objetivos que plantea la dirección, son necesarias. (Fernández, Medina, Moya y Plattini, 2003).

Amenazas a la seguridad de informaciones

Es todo aquello que pueda por ejemplo la pérdida de informaciones, de la privacidad o un fallo en los equipos físicos (Tupia, 2011).

Confidencialidad

Es la protección de información para evitar divulgaciones a entidades o individuos no autorizados. (Soriano, 2014, p. 32).

Controlamientos de seguridad informática

Para los controlamientos y gestión del sistema de seguridad informática, se efectúa la información desde el punto de vista de la seguridad, con el objetivo de identificar las actividades que se han de ejecutar y con ello establecer las directricess, los objetivos, procesos y procedimientos de seguridad en las informaciones. (Norma ISO 27002).

Disponibilidad

Significa tener accesos a la información cuando se necesita con urgencia, cualquier retraso a niveles en servicios es una violación. Si un sistema de informaciones no está disponible, como no disponer del sistema. (Soriano, 2014, p. 34).

Evaluación de la seguridad física de la información

Se estudian y evalúan los mecanismos de protección física que tiene la información, en archivo y de manera digital, los sistemas software que gestionan los datos, el hardware y su configuración, las personas involucradas, todo los descrito y demás deben estar dentro de los límites permitidos por las directricess establecidas. (Norma ISO 27000).

Evaluación de la seguridad lógica de la información

Esta evaluación se concentra en los aspectos de usabilidad que se le da a los sistemas software que se emplean en la organización, la protección de los datos, mediante mecanismos propios del software y de los sistemas gestores de base de datos, y los usuarios con sus respectivos accesos. (Norma ISO 27000)

Evaluación de la seguridad del personal que manipula la información

La evaluación de los aspectos de seguridad en el preciso instante del trabajo con la información, ya sea digital o en papel, así también de los equipos a fin de tener un adecuado uso de parte de los empleados, esto es necesario que se tome en cuenta. (Norma ISO 27000).

Evaluación de la seguridad en las informaciones y las bases de datos

La evaluación de la protección de la información debe enmarcarse dentro de los aspectos de confidencialidad, disponibilidad e integridad. Desde el momento de su acopio, la información deberá estar clasificada, a la mano de quien la desee y tenga los permisos de acceder a ella, y debe permanecer inmutable hasta que, por privilegio, un trabajador pueda cambiar la información. (Tipton& Krause, 2007).

Evaluación de la seguridad en la operación del hardware

Cuando se evalúa , se debe identificar las principales vulnerabilidades de hardware, de las cuales se pueden mencionar a continuación: Inapropiada operación, fallas en mantenimiento, inadecuada seguridad física y falta de protección contra desastres naturales. (Norma ISO 27000).

Evaluación de la seguridad en las telecomunicaciones

En las directricess de la organización deben organizar y no deben usarse para otros fines no autorizados, por seguridad y por productividad, salvo en emergencias concretas, si allí se ha especificado y, mejor dicho, para comunicaciones con voz. (Maiwald, 2005).

Gestión integral de alarmas (ERM)

Es el conjunto estructurado, que permite a las organizaciones identificar y evaluar los alarmas que puedan afectar el cumplimiento de sus objetivos. Para emprender en forma efectiva las medidas para responder ante ellos. (Mejía, 2006, p.41).

Gobierno de seguridad de informaciones

Sistema en seguridad en las informaciones de una organización son dirigidas y controladas. (Cruz y Fukusaki,2017, p.39)

Integridad

Es el cuidado de data frente a cambios y/o reordenación hecha por entidades no autorizadas. Una violación de las integridades se debe siempre a ataques en actividad. (Soriano, 2014, p. 33)

Metodología MAGERI.T.

Es método para investigar los alarmas que soportan los Sistemas de informaciones y alarmas." (Paredes, 2011, p. 109).

Metodología PMBOK

Es conjunto de habilidades, y técnicas orientadas a tareas del proyecto que cumpla con metas en el mismo. Se hace mediante integración de 47 procesos en la dirección de proyectos(PMI, 2013,p.5).

Norma ISO 31000

Permite brindar soporte a organizaciones alcanzar y utilizar recursos efectivamente para el tratamiento del alarma (ISO 3100, 2011).

Norma ISO/IEC 27005

Provee lineamientos para la gestionamiento en alarmas de seguridad en las informaciones en una organización, dando soporte en particular a los requerimientos de un Sistematización de gestionamiento de seguridaden las informaciones (SGSI) de acuerdo a la norma ISO/IEC 27002. (Norma ISO/IEC/NTP 27005).

Norma ISO/IEC 27002

Es una norma internacional dada por ISO que gestiona seguridad en las informaciones en una empresa (Kosutic, 2013).

Norma ISO/IEC 27002

Proporciona diferentes recomendacion de las practicas en la gestión de la seguridad en las informaciones a los stakeholders y responsables para iniciar, implementar sistemas de gestión de la seguridad en las informaciones. (Norma ISO/IEC 27002)

Alarmas

Es el efecto de la incertidumbre en los objetivos, donde los alarmas de seguridad en las informaciones se asocian con el potencial que amenazas exploten las vulnerabilidades de un Activo de informaciones o grupo de Activos de informaciones y por lo tanto causar daño a una organización. (Norma ISO 2700)

Alarmas identificados

Cualquier cosa que amenace el progreso de un proyecto; algo que bajo ciertas circunstancias puede interferir o interrumpir la buena marcha del proyecto. Está relacionado con algún evento que podría ocurrir y que en caso ocurriese tendría un impacto negativo para el progreso del proyecto (Llorens, 2005).

Tratamiento del alarma

Proceso en seleccionar e implementación de medidas para cambiar el alarma. (Cruz y Fukusaki, 2017, p. 39)

Vulnerabilidad

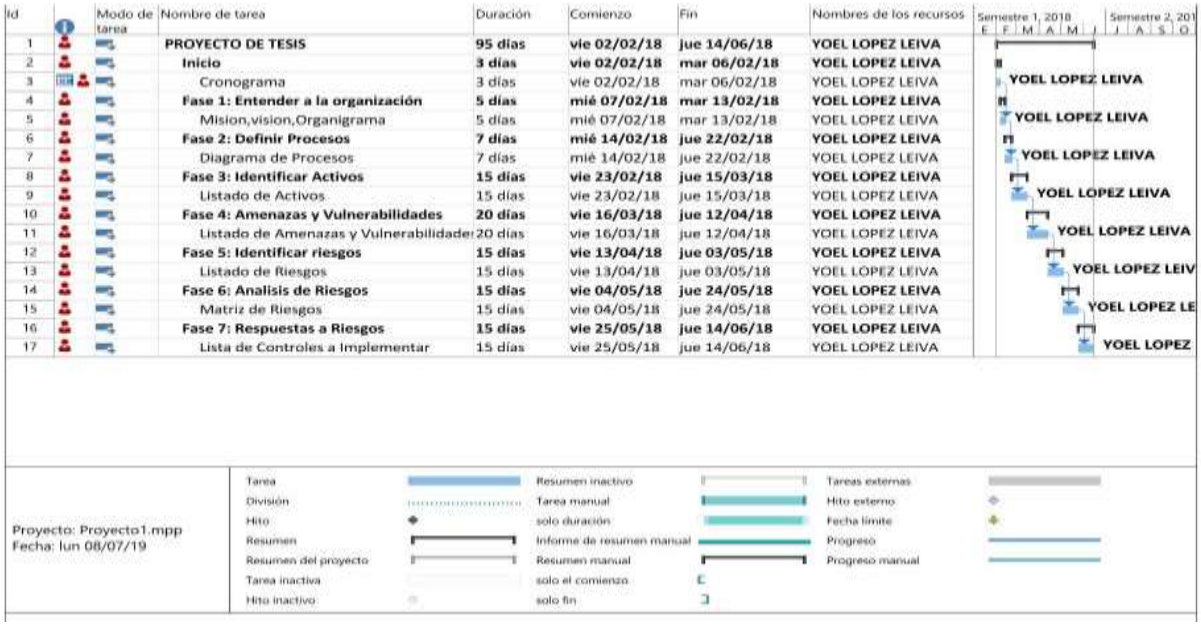
Es una debilidad asociada con los activos de la organización, las cuales pueden ser explotadas por una amenaza causando incidentes no deseados. La vulnerabilidad no causa daño, es una condición que permite que una amenaza afecte a un activo (Alexander, 2005).

CAPÍTULO 3

DESARROLLO DEL PROYECTO

3.0.-Cronograma del Proyecto. -

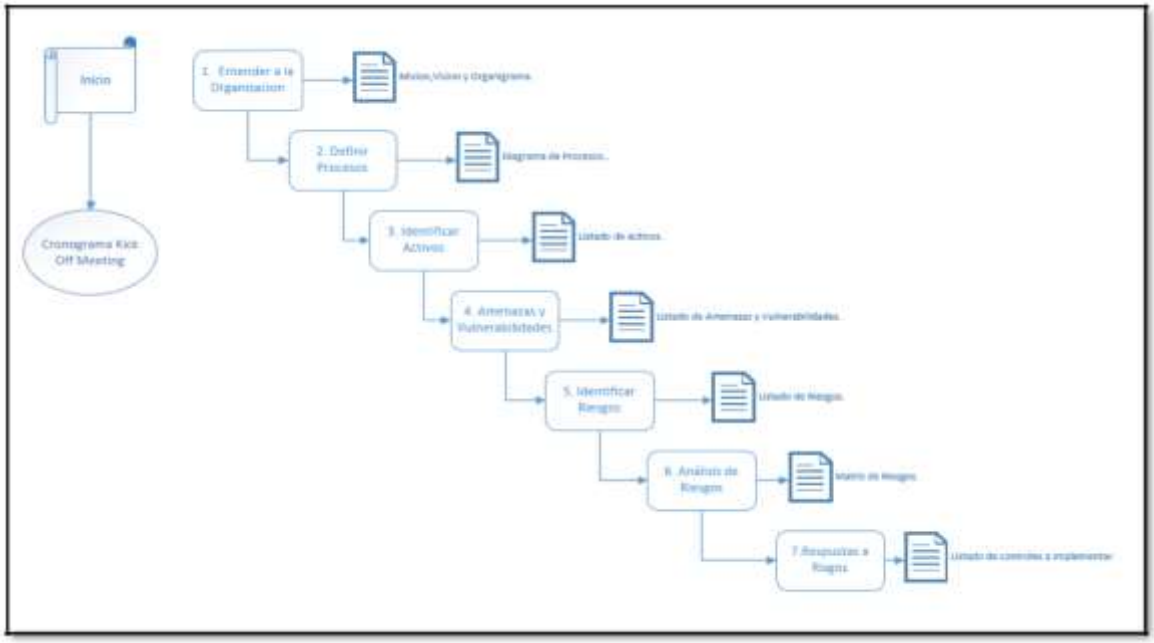
Figura 7: Cronogramas del Proyecto



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
1		**PROYECTO DE TESIS**	**95 días**	**vie 02/02/18**	**jue 14/06/18**	YOEL LOPEZ LEIVA
2		**Inicio**	**3 días**	**vie 02/02/18**	**mar 06/02/18**	YOEL LOPEZ LEIVA
3		Cronograma	3 días	vie 02/02/18	mar 06/02/18	YOEL LOPEZ LEIVA
4		**Fase 1: Entender a la organización**	**5 días**	**mié 07/02/18**	**mar 13/02/18**	YOEL LOPEZ LEIVA
5		Mision,vision,Organigrama	5 días	mié 07/02/18	mar 13/02/18	YOEL LOPEZ LEIVA
6		**Fase 2: Definir Procesos**	**7 días**	**mié 14/02/18**	**jue 22/02/18**	YOEL LOPEZ LEIVA
7		Diagrama de Procesos	7 días	mié 14/02/18	jue 22/02/18	YOEL LOPEZ LEIVA
8		**Fase 3: Identificar Activos**	**15 días**	**vie 23/02/18**	**jue 15/03/18**	YOEL LOPEZ LEIVA
9		Listado de Activos	15 días	vie 23/02/18	jue 15/03/18	YOEL LOPEZ LEIVA
10		**Fase 4: Amenazas y Vulnerabilidades**	**20 días**	**vie 16/03/18**	**jue 12/04/18**	YOEL LOPEZ LEIVA
11		Listado de Amenazas y Vulnerabilidades	20 días	vie 16/03/18	jue 12/04/18	YOEL LOPEZ LEIVA
12		**Fase 5: Identificar riesgos**	**15 días**	**vie 13/04/18**	**jue 03/05/18**	YOEL LOPEZ LEIVA
13		Listado de Riesgos	15 días	vie 13/04/18	jue 03/05/18	YOEL LOPEZ LEIVA
14		**Fase 6: Analisis de Riesgos**	**15 días**	**vie 04/05/18**	**jue 24/05/18**	YOEL LOPEZ LEIVA
15		Matriz de Riesgos	15 días	vie 04/05/18	jue 24/05/18	YOEL LOPEZ LEIVA
16		**Fase 7: Respuestas a Riesgos**	**15 días**	**vie 25/05/18**	**jue 14/06/18**	YOEL LOPEZ LEIVA
17		Lista de Controles a Implementar	15 días	vie 25/05/18	jue 14/06/18	YOEL LOPEZ LEIVA

3.1.- Metodología de Desarrollo. - La metodología realizada en el presente proyecto está basada en el PMBOK y MAGERI.T., etapas que se contemplan en el proyecto son:

Figura 8: Metodología de Desarrollo



3.1.1.-Entender a la Organización. -Podemos entender a la organización mediante su misión, visión, organigrama. A través de estos podemos conocer el fin que tienen en el mercado laboral.

- **Misión. -** Mediante esto se mide la en la empresa desde la vista general. Entre las variables se pueden ver la misión están los servicios que oferta los mercados.
- **Visión. -** En lo que pretende convertirse a largo plazo.
- **Organigrama.** - Representación en gráficos de estructura de una empresa o cualquier otra organización, que incluye en departamentos, las personas que las dirigen, hacen un esquema de relaciones jerárquicas y competenciales.

3.1.2.-Definir Procesos. - Para crear procesos en empresa se define la cadena de valores. Estos procesos que son el Core del Negocio se desarrollara en el Software Bizagi.

3.1.3.-Identificar Activos.- Se ejecuta identificar y valorar informaciones También se usa ISO/IEC 27002, y MAGERI.T., se detalla métodos de identificación y valoración. Es importante porque determina cuáles son los activos de informaciones críticos en la probabilidad de los procesos.

3.1.3.1.-Categorización de activos

Los principales activos identificados se clasificarán usando las siguientes categorías:

- **Activos de informaciones**

- Información escrita: Documentos creados y/o conservados en papel (planes, programas, estudios, informes, material de entrenamiento, contratos firmados, reportes, certificados, facturas, memos, documentos, etc.).
- Video, cintas, DVD, entre otros.
- Información por boca: conversaciones, telefónicas, presentaciones orales , medios virtuales (video conferencia).

- **Activos de software**
  - Software comercial o herramientas, utilitarios: Sistema Operativo, Office 365, u otros.
  - Software desarrollado: Sistemas Integrados, Sistema de informaciones.
  - Software de administración de Base de Datos: SQL, Oracle, DB/2, Informix, MySQL, entre otros.
  - Otro software: Software específicos desarrollados por terceros.

- **Activos de hardware**
  - Equipos de procesamiento: Servidores, computadoras y otros.
  - Equipos en telecomunicaciones: Red LAN (ruteadores, Switches), red telefonía (central teléfonos), red inalámbrica (acces point), etc.
  - Mobiliario y equipamiento: Estantes, cajas fuertes, archivadores, etc.

- **Personal**
  - Empleados: Personal interno, contratado a tiempo completo o parcial, Staff de la organización o practicantes.

Tabla 3: Activos

Tipo	Código	Categoría
Activos de informaciones	I1	Información escrita
	I2	Información electrónica
	I3	Información hablada
Activos de Software	SW1	Software herramientas y utilitarios
	SW2	Software por otros
	SW3	Software internamente desarrollado
	SW4	Software para administración de BD
	SW5	Otros softwares
Activos Físicos	F1	Equipo de procesamiento
	F2	Equipo de comunicaciones
	F3	Medio de almacenamiento
	F4	Mobiliario y equipamiento
	F5	Otros equipos
Personal	P2	Empleados

3.1.3.2.-Clasificación de activos

Esta clasificación está dada por la característica del activo que se encuentran dentro de la empresa y puede ser:

- Interno: Son todos aquellos activos que pertenecen a un proceso o área y que por su naturaleza son reservados. Su divulgación está sujeta a aprobación de gerencia y oficial de seguridad.
- Público: Son todos aquellos activos que se presumen públicos.
- Restringida: Es toda información cuyo contenido es restringido a un solo grupo determinado de individuos. Su divulgación puede constituir una ventaja competitiva o intereses privados, afectar los intereses de la organización en negociaciones en curso o revelar a terceros información clasificada.

3.1.3.3.-Estimación de valor de activos

Para obtener valores en activos promedio en sumar valores del nivel en Confidencialidad, y Disponibilidad y Integridad.

Para determinar el nivel de confidencialidad del Activo, se emplea la siguiente escala de valor.

Tabla 4: Estimación de valor de activos

Valor del Activo		**Confidencialidad**
5	Muy Alto	Cuando la pérdida o falla de un determinado activo afecta la accesible, impactando **irreversiblemente** la operatividad, lo comercial, rentabilidad o o imagen Empresarial .
4	Alto	Cuando la pérdida o falla de un determinado activo afecta la accesible, impactando **gravemente** la competitividad, el cumplimiento legal o comercial, o imagen Empresarial .
3	Medio	Cuando la pérdida o falla de un determinado activo afecta la accesible y disposición informacional, impactando **considerablemente** la operacionalidad, competición, el cumplimiento legal o comercial, o imagen Empresarial.

2	Bajo	Cuando la determinado activo afecta la accesible, impactando **parcialmente** competitividad, comercial, rentabilidad o o imagen Empresarial .
1	Muy Bajo	Cuando la falla de un determinado activo afecta la accesible y disposición de la información, **no impactando** las operaciones, competencia, cumplimiento legal y/o comercial, rentabilidad o o imagen Empresarial .

Valor del Activo		**Integridad**
5	Muy Alto	Cuando falla de un determinado activo afecta la accesible y impactando **irreversiblemente** la operatividad o imagen Empresarial.
4	Alto	Cuando la pérdida de un determinado activo afecta la accesible y, impactando **gravemente** la competitividad, el cumplimiento legal o comercial, o imagen Empresarial.
3	Medio	Cuando falla de un determinado activo afecta la accesible, impactando **considerablemente** la operacionalidad, el cumplimiento legal o comercial, rentabilidad de la Empresa.
2	Bajo	Cuando la falla de un determinado activo afecta la accesible, impactando **parcialmente** competitividad, el cumplimiento legal o comercial, rentabilidad o imagen Empresarial.
1	Muy Bajo	Cuando la falla de un determinado activo afecta la accesible y disposición de la información, **no impactando** las operaciones, competencia, cumplimiento legal y/o comercial, rentabilidad o o imagen Empresarial.

Valor del Activo		Disponibilidad
5	Muy Alto	La pérdida de un determinado activo impacta la accesible y disposición de información, impactando **irreversiblemente** la operacionalidad, lo comercial, rentabilidad de la Empresa.
4	Alto	Cuando la pérdida o falla de un determinado activo afecta la accesible y disposición de la información, impactando **gravemente** el cumplimiento legal o imagen Empresarial.
3	Medio	Cuando pérdidas de un determinado activo afecta la accesible , impactando **considerablemente** la operacionalidad, competición, el cumplimientos legales o comercial, rentabilidad o imagen de la Empresa.
2	Bajo	Cuando la de la accesible y **parcialmente** competitividad, lo comercial, rentabilidad o imagen de la Empresa.
1	Muy Bajo	Cuando la falla de un determinado activo afecta la accesible y dispensa de información, **no impactando** las operaciones, competencia, cumplimiento legal y/o comercial, rentabilidad o imagen de la Empresa.

3.1.3.4.-Determinación de la apreciación del activo

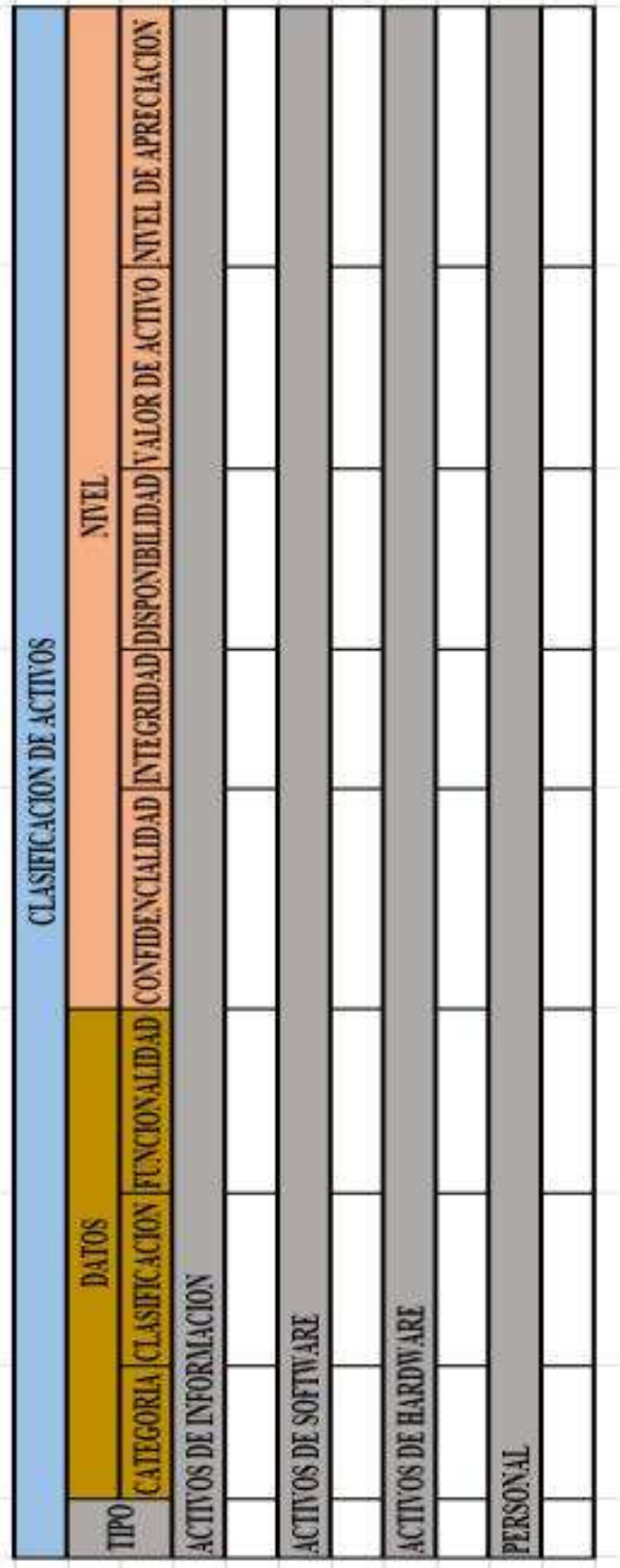
Para determinar la apreciación del activo, se identifica el Valor del Activo dentro del rango de apreciación (Alto: Rojo, Medio: Amarillo y Bajo: Verde).

Tabla5: Determinación de la apreciación activo

Valor Activo	Apreciación
3.5 – 5	Alto
1.5 - 3.5	Medio
1 - 1.5	Bajo

El equipo de trabajo se encargará de completar el siguiente formato adjunto, teniendo encuentra los puntos expuestos anteriormente.

Tabla 6: Clasificación de activos



CLASIFICACION DE ACTIVOS							
TIPO	DATOS			NIVEL			
	CATEGORIA	CLASIFICACION	FUNCIONALIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DE ACTIVO	NIVEL DE APRECIACION
ACTIVOS DE INFORMACION								
ACTIVOS DE SOFTWARE								
ACTIVOS DE HARDWARE								
PERSONAL								

3.1.4.-Amenazas y Vulnerabilidades. - Una amenaza es un evento no estimado que pueda causar daño a los activos de informaciones. Las amenazas se clasifican en:

- Amenazas de naturaleza: maremotos, inundaciones.
- Amenazas en instalaciones: explosión, fallas en la mecanica.
- Amenazas de humanos: ingeniería social, falta de trabajadores clave.
- Amenazas en tecnológia: virus, hacking, de conectividad.

Una Vulnerabilidad es cualquier debilidad en los controlamientos de protección de los activos dentro del centro de datos que puedaaceptar amenazas causarle daños y producir pérdidas en la empresa. Las falencias se clasifican en:

- Seguridad de rrhh: Falta entrenamiento de conciencia preventiva de seguridad, falta mecanismos monitoreo, falta directricess en uso de telecomunicaciones, no borrar accesos términos de contratos de trabajo.
- Control de acceso: Segregación inapropiada de redes, falta de directrices sobre escritorio y pantalla limpia, directrices incorrectas.
- Seguridad física y ambiental: Control en accesos físico inadecuado a oficinas, salones y edificios, ubicación en, almacenes desprotegidos, carencia de programas para sustituir equipos.
- Administración de las operaciones y comunicaciones: Complicadas interfaces para clientes, , falta, carencia tareas segregadas, , falta de protección en redes de conexión.
- Adquisición, desarrollo y mantenimiento de sistemas de informaciones: Protección de llaves criptográficas, directricess de validaciones en data procesada, carencias de ensayos de software, sin documentación de software, malos ensayos de data.

3.1.4.1.-Nivel de Vulnerabilidad y Nivel de Amenaza

En la determinación del nivel en vulnerabilidades, se evalúa y se identifica el nivel de capacidad de los controlamientos de protección existentes (Preventivos, Defectivos y Correctivos). Se estima el nivel de vulnerabilidad usando la siguiente formula:

$$\frac{(\quad)+(\quad)+(\quad)}{3}$$

Para determinar el nivel de Capacidad (NC) que los controlamientos de protección existentes poseen, se usará la siguiente tabla:

Tabla 7: Niveles de Capacidades

	Valor		Descripción
	5	Incompleto	Controles no implantado conseguir su objetivo
	4	Realizado	Controles Implantado logra su objetivo definido (no documentado)
	3	Gestionados	La ejecución del controles gestió y control
	2	Definidos	La ejecución del controles definido por la Empresa
	1	Predecibles	La ejecución de los controlamientos de la recopilaciones y análisis en la eficacia de los controlamientos.

Para calcular el nivel de amenaza, se promedia usando los valores del nivel de impacto y frecuencia que estos tendrán dentro de los activos TI que se manejan dentro del centro de datos. Se usará la siguiente fórmula para calcular el nivel de amenaza:

$$\frac{+}{2}$$

Para identificar el nivel de impacto y frecuencia de las amenazas se usará las siguientes tablas de valores:

	Valor		Descripción
Nivel de Impacto	5	Muy Alta	Impactaría irreversiblemente
	4	Alta	Impactaría gravemente
	3	Media	Impactaría considerablemente
	2	Baja	Impactaría parcialmente
	1	Muy Baja	No impactaría

Frecuencia de Amenaza	Valor	Descripción
	5	Muy Alto	Vez en semana
	4	Alto	Vez en mes
	3	Medio	Vez en 6 meses
	2	Bajo	Vez al año
	1	Muy Bajo	Vez en 5 años

3.1.4.2.-Probabilidad en ocurrencia y nivel de ocurrencia

Se estima la probabilidad de ocurrencia de la media de sumar valores de niveles de vulnerabilidades y niveles de amenazas:

$$. . = (\frac{}{+ \quad)2}$$

Para determinar el nivel de ocurrencia, se identifica el valor de la probabilidad de ocurrencias dentro del rango de nivel de ocurrencias establecido (Alta: Rojo, Media: Amarillo y Baja: Verde)

Probabilidad en Ocurrencia	Nivel de Ocurrencia
3.5 - 5	Alto
1.5 - 3.5	Medio
1 - 1.5	Bajo

El equipo de seguridad completara el siguiente formulario y usara los valores explicados anteriormente para tener probabilidades de ocurrencias y los niveles de vulnerabilidad y amenaza.

Tabla 8: Análisis amenazas

N°	ACTIVOS TI ANÁLISIS DE	AMENAZAS AFECTADOS

		AMENAZA	DESCRIPCIÓN	NIVEL DE IMPACTO AMENAZA	FRECUENCIA DE LA AMENAZA	NIVEL DE AMENAZA

Tabla 9: Análisis de Vulnerabilidad

N°	ACTIVOS TI AFECTADOS	ANALISIS DE VULNERABILIDAD					
		CONTROLAMIENTOS PREVENTIVOS (NC)	CONTROLAMIENTOS DETECTIVOS (NC)	CONTROLAMIENTOS CORRECTIVOS (NC)	CLASIFICACIÓN DE VULNERABILIDADES	NIVEL DE VULNERABILIDAD	

Tabla 10: Análisis de probabilidad de ocurrencia

ANÁLISIS DE PROBABILIDAD DE OCURRENCIA					
N°	ACTIVOS TI AFECTADOS	NIVELES		OCURRENCIA	
		NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	PROBABILIDAD	NIVEL

3.1.5.-Identificar Alarmas. - Relacionadas ya, la vulnerabilidad y amenaza con activos de informaciones se inicia el alarma y sus consecuencias, del alarma, determinan criticidad es: Probabilidad y el impacto.

3.1.5.1.-Nivel de Impacto.-Para calcular el nivel de impacto, se usa el promedio de los valores del impacto económico y operacional según la formula adjuntada.

Para calcular el nivel de impacto económico y operacional se usará las siguientes tablas:

Tabla 11: Nivel de impacto económico

	Valor		Descripción
Nivel de Impacto Económico	5	Muy Alto	Mermas superiores a los S/. 150,000
	4	Alto	Mermas superiores a los S/. 45,000 y menores que los S/. 150,000
	3	Medio	Mermas superiores a los S/. 20,000 y menores que los S/. 45,000
	2	Bajo	Mermas mayores a los S/. 8,000 y menores que los S/. 20,000
	1	Muy Bajo	Mermas menores a los S/. 8,000

Tabla 12: Nivel de impacto operacional

	Valor		Descripción
	5	Muy Alto	Impacta irreversible operacional de procedimientos de Empresa
	4	Alto	Impacta enormemente operatividad de procedimientos de Empresa
	3	Medio	Impacta seriamente operatividad de procedimientos de la Empresa

	2	Bajo	Impactaparcialmenteoperatividad de procedimientos de la Empresa
	1	Muy Bajo	No Impacta operatividad de los procedimientos de la Empresa

3.1.5.2.- Nivel de exposición del alarma y nivel del alarma

Para calcular el nivel de exposición de alarmas, se usa la media de valores del valor de activos, nivel de impacto y probabilidad en ocurrencias según la formula adjuntada.

Para determinar el nivel de alarma, se calcula el valor del nivel de exposición al alarma dentro del rango de nivel de alarma establecido (Muy Alto: rojo; Alto: anaranjado; Medio: amarillo y Bajo: verde).

Tabla 13: Nivel de probabilidad ocurrencias

		Nivel de Impacto				
		5. Muy Alto	4. Alto	3. Medio	2. Bajo	1. Muy Bajo
Probabilidad de Ocurrencia	5. Muy Alto	Muy Alto	Muy Alto	Alto	Alto	Medio
	4. Alto	Muy Alto	Alto	Alto	Medio	Bajo
	3. Medio	Alto	Alto	Medio	Medio	Bajo
	2. Bajo	Alto	Medio	Medio	Bajo	Bajo
	Bajo	Medio	Bajo	Bajo	Bajo	Bajo

Tabla 14: Nivel Alarma inherente

Nivel Alarma Inherente	Descripción
Bajo	El alarma no causa un efectos en la información de la organización ni en el proceso
Medio	El alarma no causa un efecto considerable en la información de la organización, pero si en alguna actividad del proceso
Alto	El alarma puede afectar considerablemente la información, ocasionando incumplimiento de metas, pérdidas

	económicas importantes, teniendo un efecto negativo en el proceso.
Muy Alto	El alarma puede afectar seriamente la información de la organización, ocasionando incumplimientos críticos de servicio al cliente con pérdidas económicas muy importantes y daño considerable a imagenes de la institución.

Tabla 15: Identificación de alarma

IDENTIFICACION DE ALARMA									
N	S [illegible] os	[illegible] a	IMPACTO			[illegible] e l a	Valor del Activo	Alarma Efectivo	
			Impacto Económico	Impacto Operacional	Nivel de impacto			Nivel de exposición al Alarma	Nivel de Alarma

3.1.6.-Análisis de Alarmas.- El análisis cuantitativo emplea como principal herramienta de trabajo la econometría. La cuestión que se utiliza análisis cuantitativo para de medir, o valorar.

3.1.7.-Respuesta a Alarmas.- Después de que los alarmas han sido identificados y evaluados como en estado crítico, el siguiente proceso es identificar y evaluar las diferentes acciones más apropiadas para tratar los alarmas. La decisión debe ser tomada con base en los activos de TI de alto valor involucrado y su respectivo impacto en la empresa. También es importante considerar el nivel de alarma residual (aceptable) que fue identificado siguiendo los controlamientos apropiados basados en NTP-ISO/IEC 27002.

3.1.7.1.- Nivel de Tolerancia. - Se estima el Nivel de Tolerancia al Alarma del promedio de sumas de valores a nivel de Valor de Activo, a nivel en Probabilidades de Ocurrencias de Alarmas y el Nivel a Impacto; en otras palabras, el Nivel de Tolerancia es Igual a Nivel de Exposición del Alarma:

= ó

Nivel de exposición al Alarma Inherente	Nivel de Tolerancia
0 -4	Bajo
5 - 9	Medio
10 - 16	Alto
17 - 25	Muy Alto

	Sigla	Nombre	Descripción
Costo	4	Corto plazo	Mayor a S/. 1’000,000
	3	Mediano plazo	S/. 300,000 a S/.1’000,000
	2	Largo plazo	S/. 15,000 a S/. 300,000
	1	Desconocido	Menor a S/.15,000
	D	Desconocido	-

3.1.7.2.- Evaluacion del Tratamiento.- Para las amenazas que hayan obtenido un nivel de alarmas:

- Indicar la data de la amenaza, probabilidad en ocurrencia, impacto, nivel de alarma, valor del activo y nivel de tolerancia.
- Determinar el tipo de tratamiento para tratar el alarma.
- Si la estrategia es Reducir y/o Evitar el Alarma se deberá proponer uno o más mecanismos de protección por cada amenaza y describir brevemente en qué consiste.
- Identificar el tipo de control que corresponde al cumplimento de la ISO/IEC 27002. Tabla 16: Tipo de tratamiento

	Sigla	Nombre	Descripción
Tipo de Tratamiento	A	Aceptar	No hacer nada, aceptar el alarma tal como se presenta
	R	Reducir	Minimizar impactos y probabilidades en ocurrencia
	E	Evitar	Reducir la mínima posibilidad en ocurrencia de amenazas
	T	Transferir	Transfiere el impacto de la amenaza a un tercero.

Tabla 17: Costo aproximado

Tabla 18: Anexo A . ISO/IEC/NTP 27002

Anexo A - ISO/IEC 27002	
A.5.	Directrices en seguridad
A.7	Administración en recursos
A.8	Seguridad en rrhh
A.9	Seguridad en físico y entorno
A.10	Administrar omunicaciones y operatividad
A.11	Control en accesos
A.12	Adquirir sistemas de informaciones, desarrollo y mantenimiento
A.13	Administración de incidencias en seguridad
A.14	Administración de continuidad en negocios
A.15	Cumplimientos legal, técnico y auditorias

- Determinar el costo aproximado de la implementación del mecanismo propuesto usando la tabla de costo aproximado.
- Determinar el tiempo aproximado del desarrollo o implantación del mecanismo propuesto usando la tabla de tiempo aproximado:

Tabla 19: Tiempo en aproximación

Aproximado	Sigla	Nombre	Descripción
1 0	C	Corto aplazamiento	Menor de tres (03) meses
	M	Mediano	De tres (03) a doce (12) meses
	L	Largo aplazamiento	Más de (01) año
	D	Desconocido	-

- Se reevalúa el nivel de vulnerabilidad, la probabilidad que ocurra del alarma y el nivel de impacto, pero considerando que el mecanismo de protección (controlamientos) propuestos han sido implantados. De esta manera se obtiene el nivel de exposición al alarma de cada una de las opciones propuestas que nos permitirá detectar qué tan efectivo es para su implantación.

N°	Activos Afectado	Amenazas	ALARMA INHERENTE					Tipo de tratamiento	Controlamientos de protección propuestos	Observaciones	Cumplimiento del Control - ISO/IEC/NTP 27002	Precio Aprox.	Tiempo Aprox.
			Nivel de impacto	P.O. Alarma	Valor del Activo	N.E del Alarma	Nivel de Tolerancia						

3.2.- FASE 1: Entender a la Organización

La misión, visión, reglamentación y requisitos de organización se ha determinado los objetivos en los cuales se desarrolla Implementación de metodologías para gestionar los

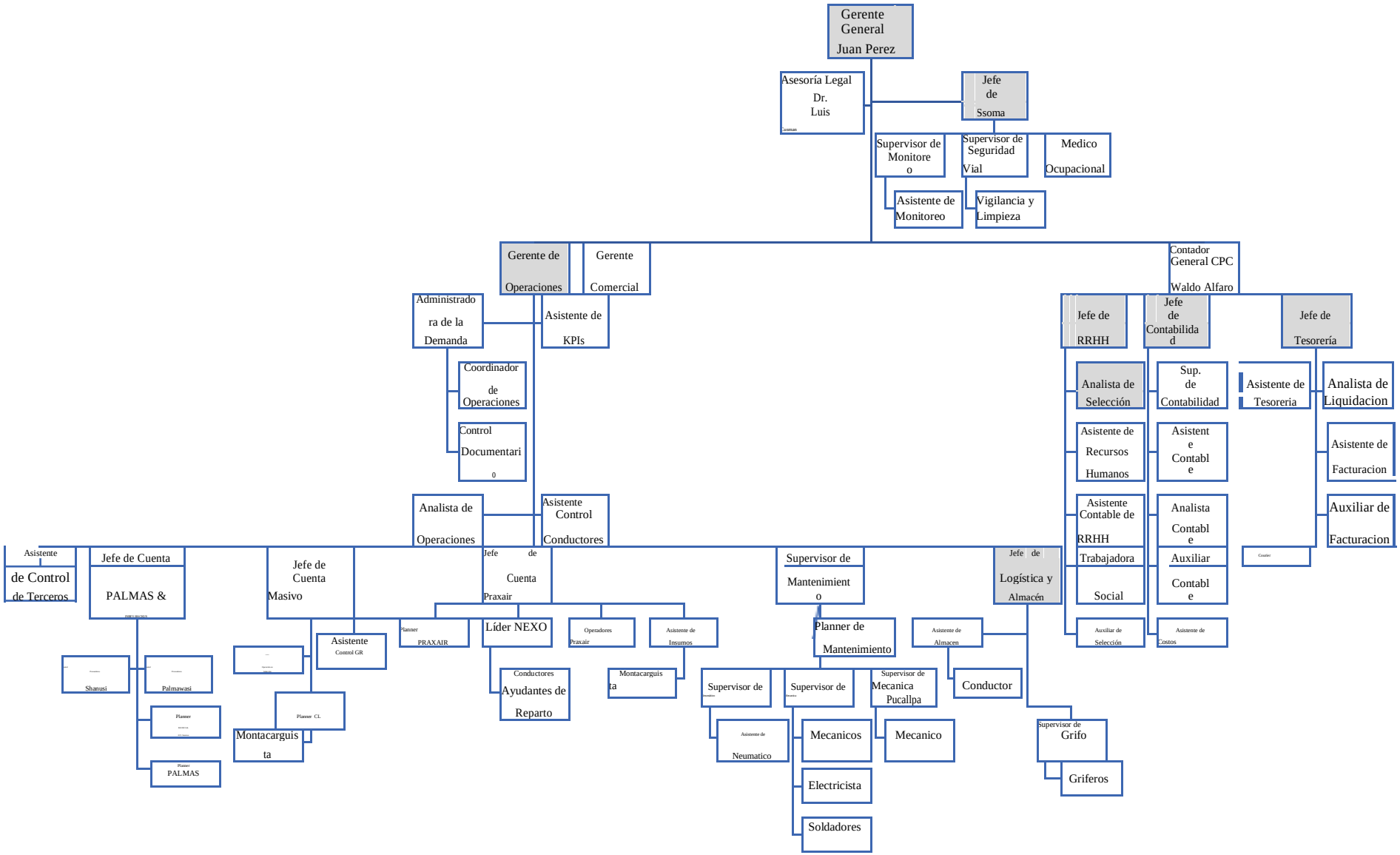
alarmas en el procesos de “Selección e Iniciacion de Personal Administrativo y Conductor” en la Empresa JP LOGISTICA SAC.

Misión, Visión y Valores de JPLOGÍSTICAS.A.C.

<table>
<tr><th colspan="2">JP LOGISTICA SAC</th></tr>
<tr><th>MISIÓN</th><th>VALORES</th></tr>
<tr><td>Satisfacer plenamente las expectativas y requisitos de nuestros clientes, brindando soluciones logísticas integrales, garantizándoles un servicio de excelencia en calidad de tiempo, seguridad, costos y cuidado ambiental.</td><td rowspan="3">Responsabilidad: En JP LOGÍSTICA cumplimos las obligaciones y los compromisos adquiridos por la empresa y clientes, dando respuestas adecuadas a los que se espera.
Respeto: Tenemos presente el valor propio y el ser y la dignidad de otros, para comprender y aceptar, dejándo actuación, es tolerante para ellos, con su condición y con relación que establecido con nosotros.
Laboriosidad: Nosotros creemos en la realización del trabajo con dedicación, orden y constancia, para que se cumplan los resultados.
Lealtad: Dar fidelidad a la misión, filosofía y valor a la organizacion en desempeño diario e invertir en talento y esfuerzo en logros de los objetivos , por medio de funciones, proyectos y tareas particulares de trabajo.
Trabajo en equipo: En JP LOGÍSTICA la organización de una forma determinada es base fundamental para lograr los objetivos en común.
Constancia: No dejarse llevar por la variedad de ideas o sentimientos, ni dejarse vencer por las dificultades, para trabajar con estabilidad y firmeza es el objetivo de JP LOGÍSTICA.</td></tr>
<tr><th>VISIÓN</th></tr>
<tr><td>Empresa líder y número uno de los servicios de operaciones Logísticas a nivel nacional, satisfaciendo a los clientes y creando el mejor ambiente laboral para que nuestros colaboradores puedan cumplir sus objetivos.</td></tr>
</table>

JP LOGISTICA SAC
OBJETIVOS DE LA EMPRESA
• Inventariar y Clasificar los Activos del Proceso de “Selección al Personal Administrativo y Conductor” • Identificar y Clasificar los Alarmas para el Proceso de “Selección al Personal Administrativo y Conductor” • Establecer Controlamientos para el Tratamiento de los Alarmas identificados en el Proceso “Selección al Personal Administrativo y Conductor”

ORGANIGRAMA DE JPLOGÍSTICAS.A.C.

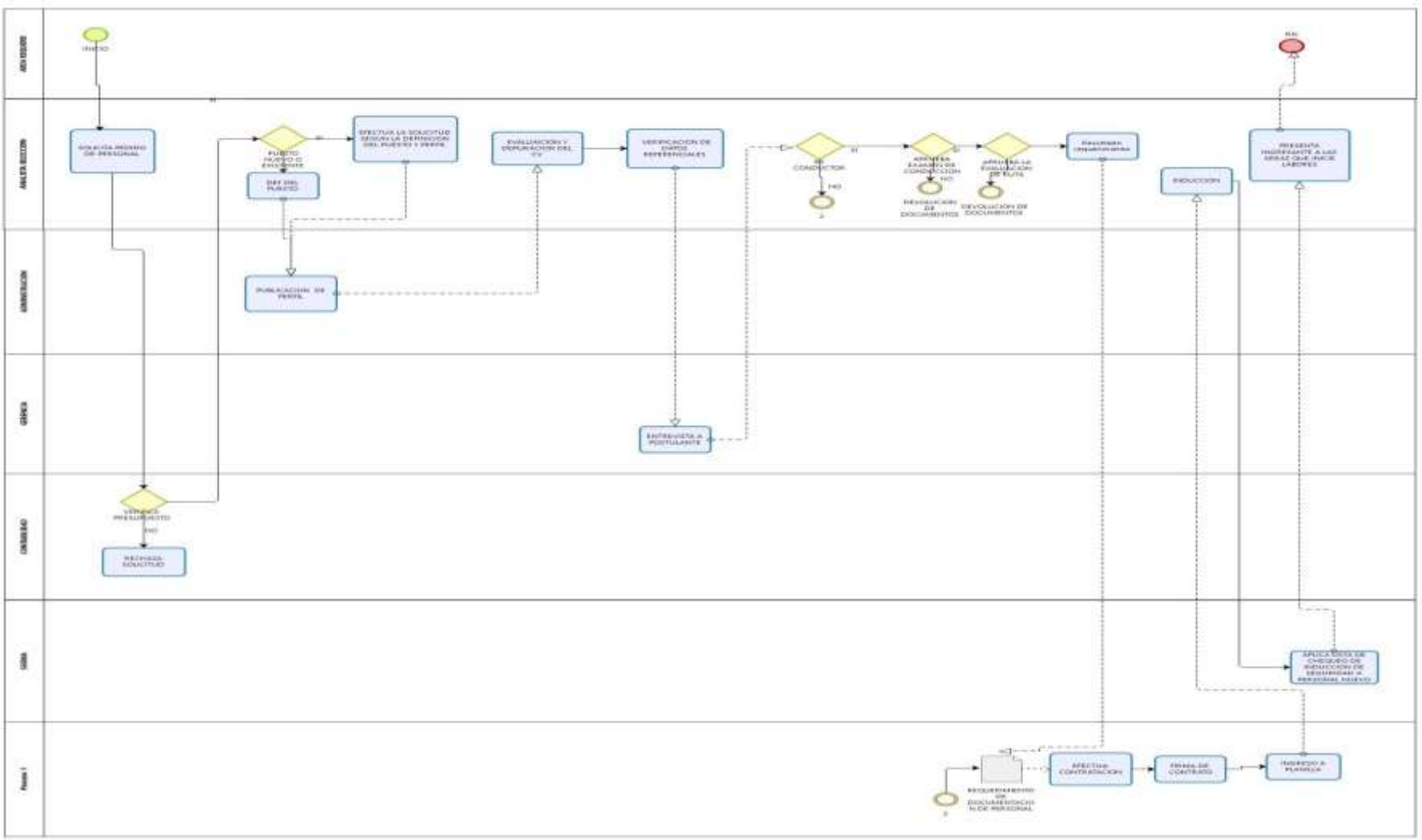


3.3.- FASE 2: Definir Proceso

Descripción: Para nuestro proceso crítico “Selección e Inducción del Personal Administrativo y Conductor”, se contempla las siguientes áreas:

- Área Solicitante: Todas las Áreas, todos los usuarios de la empresa
- Área de R.R.H.H: Análisis de Selección e Inducción
- Área de Administrativa: Gerencia de Operaciones
- Jefe de Áreas: Jefe Área Solicitante
- Área de Contabilidad: Jefe en Contabilidad
- Área de SSOMA: Jefe en Seguridad Ocupacional y Ambiente

Identificar Proceso Crítico: Selección e Inducción del Personal Administrativo y Conductor.



3.4.- FASE 3: Identificación de Activos

Tabla 20: Identificación activos

CLASIFICACIÓN DE ACTIVOS DE TI								
ACTIVO	DATOS			NIVEL DE PILARES DE SI			ACTIVOS DE TI	
	CATEGORIA	CLASIFICACIÓN	FUNCIONALIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DE ACTIVO	NIVEL DE APRECIACION
ACTIVOS DE INFORMACIONES								
Listado en Personal Administrativo y Conductor.doc	Información escrita	Restringida	El que será evaluado y el profesional en dicha especialidad	4	4	4	**4**	**Alto**
Prueba de conducción.doc	Información escrita	Interno	Considera recuperación al encandilamiento, entre la aceleración y el frenado.	4	4	4	**4**	**Alto**
Devolución de documentos.doc	Información escrita	Interno	Prueba fallida sobre el conductor o postulante a este puesto.	4	4	5	**4.3**	**Alto**

Evaluación ruta.doc	Información escrita	Interno	Prueba de ruta largas y cortas, tiempos de reacción del conductor.	3	3	4	**3.3**	**Medio**
Devolución de documentos.pdf	Información escrita	Interno	Prueba fallida sobre el conductor o postulante a este puesto.	3	4	2	**3**	**Medio**
Requerimiento de documentos personales.pdf	Información escrita	Interno	Esta gestión requiere de los documentos personales de dicho conductor dependiendo si aprobó o no la funcionalidad de prueba de conducción.	4	4	5	**4.3**	**Alto**
Firma contrato.doc	Información escrita	Interno	El contrato es el acuerdo entre empresa y trabajador, que vincula legalmente, y que brinda seguridad y protección , pues establece términos y condiciones de la relación , así como los derechos y obligaciones.	5	5	3	**4.3**	**Alto**

Ingresa a planilla.doc	Información escrita	Interno	Ingreso planillas en pago es una contabilidad a tratar. Brindan elementos que permiten demostrar su pago y los beneficios.	5	5	2	**4**	**Alto**
Inducción.pdf	Información escrita	Interno	La iniciacion es un proceso basado en conocimiento a través de la indagación, situaciones particulares a fin de originar conclusiones.	2	4	3	**3**	**Medio**
Entrevista al postulante.pdf	Información hablada	Interno	Es reunión de personas para tratar asuntos profesionales de negocios con el formato de preguntas para áreas.	2	4	3	**3**	**Medio**

Verificación de datos referenciales.pdf	Información escrita	Interno	Verificación de datos personales de dicho conductor o postulante. Es primordial para confirmar la veracidad de las referencias o por el contrario prescindir de un candidato por no haber sido del todo sincero, verificación de documentos.	2	4	3	**3**	**Medio**
Depuración de Currículos.doc	Información electrónica	Interno	Depuración y eliminación de CV que ya no están a la disposición o que ya no cumplan con los requisitos del puesto.	3	4	3	**3.3**	**Medio**
Publicación de perfil.doc	Información electrónica	Público	Publicación del perfil del puesto al que se están postulando. Mediante una publicación vía internet o correo (corporativo, Gmail, etc.)	2	3	4	**3**	**Medio**
Puesto nuevo o existente.doc	Información electrónica	Interno	Verificación del puesto si existe o no mediante un correo preguntando al administrador del puesto existente en caso contrario informaran que el puesto no existe.	3	3	3	**3**	**Medio**

Efectúa la solicitud según el puesto perfil.doc	Información escrita	Interno	Efectúa y verifica el personal según como requiere el área solicitante, mediante correos electrónicos o documentos (CV).	4	4	4	**4**	**Alto**
Verifica presupuesto.doc	Información electrónica	Interno	El área de contabilidad hace la verificación si cumplen con los requisitos para dicho beneficio del conductor o colaborador.	2	3	4	**3**	**Medio**
Solicita pedido de personal.pdf	Información electrónica	Interno	Un pedido de empleos es solcitud de contacto que envía una organizacion en la que se desea ingresar a trabajar. La persona interesada debe explicar, es el motivo de contacto y detalle aptitudes y experiencia , etc. mediante presencial o correo electrónico.	4	4	4	**4**	**Alto**
Requerimiento de documentos personales.pdf	Información electrónica	Interno	Una vez pasada la evaluación y aceptada la oferta se pasa al siguiente requerir los documentos de dicho postulante.	2	3	4	**3**	**Medio**
Rechaza.doc	Información electrónica	Público	Prueba fallida sobre el conductor o postulante a este puesto.	2	4	3	**3**	**Medio**
ACTIVOS DE SOFTWARE								

Windows 10 Pro de RRHH	Información electrónica	Interno	Sistema operativo, plataforma por el cual el usuario interactua, por el cual genera archivos con contienen informacion valiosa para la empresa	4	4	3	3.7	Alto
Windows 10 Pro de Area Solicitante	Información electrónica	Interno	Sistema operativo, plataforma por el cual el usuario interactua, por el cual genera archivos con contienen informacion valiosa para la empresa	4	4	3	3.7	Alto
Windows 10 Pro Area de Almacen	Información electrónica	Interno	Sistema operativo, plataforma por el cual el usuario interactua, por el cual genera archivos con contienen informacion valiosa para la empresa	4	4	3	3.7	Alto
Windows 10 Pro Area de Contabilidad	Información electrónica	Interno	Sistema operativo, plataforma por el cual el usuario interactua, por el cual genera archivos con contienen informacion valiosa para la empresa	4	4	3	3.7	Alto
Windows 10 Pro del Area de SOMA	Información electrónica	Interno	Sistema operativo, plataforma por el cual el usuario interactua, por el cual genera archivos con contienen informacion valiosa para la empresa	4	4	3	3.7	Alto

Windows Server 2016	Información electrónica	Interno	Sistema operativo, plataforma por el cual el usuario interactua, con el que gestiona y distribuye la informacion valiosa de empresa a los usuarios, genera archivos con contienen informacion valiosa para la empresa	5	5	2	4	Alto
Microsoft Oficce 2016	Información electrónica	Interno	Programa por el cual se generan archivos, cuadros, presentaciones, documentos para la empresa que contienen informacion valiosa.	3	3	4	3.3	Medio
Eset Antivirus	Información electrónica	Interno	Programa creado especialmente para poder evitar infectar nuestro equipo PC de virus, malware, troyanos, etc, proteger informacion valiosa para la empresa	5	5	1	3.7	Alto
Active Directory	Información electrónica	Interno	Programa creado especialmente para poder evitar infectar nuestro equipo PC de virus, malware,	5	5	1	3.7	Alto

			troyanos, etc, proteger informacion valiosa para la empresa					
Usuario Red RRHH	Información electrónica	Interno	Activo de Seguridad para acceso al equipo	5	5	1	3.7	Alto
Usuario de Red Solicitante	Información electrónica	Interno	Activo de Seguridad para acceso al equipo	5	5	1	3.7	Alto
Usuario de Red Almacen	Información electrónica	Interno	Activo de Seguridad para acceso al equipo	5	5	1	3.7	Alto
Usuario de Red Contabilidad	Información electrónica	Interno	Activo de Seguridad para acceso al equipo	5	5	1	3.7	Alto
Usuario de Red SOMA	Información electrónica	Interno	Activo de Seguridad para acceso al equipo	5	5	1	3.7	Alto
Correo Corporativo RRHH	Información electrónica	Interno	Activo para la comunicación interna y externa	5	5	1	3.7	Alto
Correo Corporativo Area Silicitante	Información electrónica	Interno	Activo para la comunicación interna y externa	5	5	1	3.7	Alto
Correo Corporativo Almacen	Información electrónica	Interno	Activo para la comunicación interna y externa	5	5	1	3.7	Alto

Correo Corporativo Contabilidad	Información electrónica	Interno	Activo para la comunicación interna y externa	5	5	1	3.7	Alto
Correo Corporativo SOMA	Información electrónica	Interno	Activo para la comunicación interna y externa	5	5	1	3.7	Alto

ACTIVOS HARDWARE								
Servidor Central AD	Información electrónica	Restringida	Equipo especial para la funcionabilidad de servidores para labores pesadas, de horas de trabajo continuas.	1	1	2	1.3	Bajo
Computadora de RRHH	Información electrónica	Público	Equipo especial para la funcionabilidad de sistemas operativos(windows 10), para la labor del usuario.	2	1	1	1.3	Bajo
Computador del Area solicitante	Información electrónica	Interno	Equipo especial para la funcionabilidad de sistemas operativos(windows 10), para la labor del usuario.	2	1	1	1.3	Bajo
Computador del Area Almacen	Información electrónica	Interno	Equipo especial para la funcionabilidad de sistemas operativos(windows 10), para la labor del usuario.	2	1	1	1.3	Bajo
Computador del Area Contabilidad	Información electrónica	Interno	Equipo especial para la funcionabilidad de sistemas	2	1	1	1.3	Bajo

			operativos(windows 10), para la labor del usuario.					
Computador del Area SOMA	Información electrónica	Interno	Equipo especial para la funcionabilidad de sistemas operativos(windows 10), para la labor del usuario.	2	1	1	1.3	Bajo
Linea de Internet	Información electrónica	Interno	Equipo especial para la funcionabilidad de sistemas operativos(windows 10), para la labor del usuario.	2	1	1	1.3	Bajo
Equipo Firewall	Información electrónica	Interno	Equipo especial para la funcionabilidad de sistemas operativos(windows 10), para la labor del usuario.	2	1	1	1.3	Bajo
Cableado Estrcturado	Información electrónica	Público	Equipo especial para la funcionabilidad de sistemas operativos (windows 10), para la labor del usuario.	2	1	1	1.3	Bajo
SWITCH TPLINK DE 24 PUERTOS	Información electrónica	Restringida	Dispositivo para la distribucion de cableado/conectividad de cada	1	2	1	1.3	Bajo

			equipo (PC), distribucion de la informacion					
SWITCH TPLINK DE 16 PUERTOS	Información electrónica	Restringida	Dispositivo para la distribucion de cableado/conectividad de cada equipo (PC), distribucion de la informacion	2	1	1	1.3	Bajo
Marcador Digital	Información electrónica	Restringida	Equipo de control de Asistencia para trabajadores Interno de la Empresa	2	1	1	1.3	Bajo

PERSONAL								
Psicologo	Información hablada	Interno	Personal especializado para el filtro de la selección de personal requerido para el area solicitante.	2	1	1	1.3	Bajo
Personal RRHH	Información hablada	Interno	Personal especializado para el filtro de la selección de personal requerido para el area solicitante.	2	1	1	1.3	Bajo
Personal Almacen	Información hablada	Interno	Personal especializado para el filtro de la selección de personal requerido para el area solicitante.	2	1	1	1.3	Bajo
Personal de Area Requermiento	Información ablada	Interno	Personal especializado para el filtro de la selección de personal requerido para el area solicitante.	2	1	1	1.3	Bajo
Administrador	Información hablada	Interno	Personal especializado para el filtro de la selección de personal requerido para el area solicitante.	2	1	1	1.3	Bajo
Personal de SOMA	Información hablada	Interno	Personal especializado para el filtro de la selección de personal requerido para el area solicitante.	2	1	1	1.3	Bajo

3.5.- FASE 4: Amenazas y Vulnerabilidades. -

Tabla 21: Amenazas y vulnerabilidades

N°	ACTIVOS TI AFECTADOS	ANALISIS DE AMENAZAS				
		AMENAZAS	DESCRIPCION	Nivel de Impacto	Frecuencia de la Amenaza	Nivel de Amenaza
1	Listado de Conductor	Amenazas humanas	Modificacion de ficha de documentos del conductor	5	2	3.5
2	Prueba de conduccion	Amenazas humanas	Modificacion de ficha de documentos del conductor	5	4	4.5
3	Devolucion de documentos	Amenazas tecnológicas	Perdida de documentos o fichas mal llenadas	4	3	3.5
4	Evaluacion ruta	Amenazas humanas	Informacion Alterada o erronea del conductor	2	2	2
5	Devolucion de documentos	Amenazas humanas	Informacion Alterada o erronea del conductor	4	2	3

6	Requerimiento de documentos personales	Amenazas humanas	Informacion Alterada o erronea brindada por el conductor	3	2	2.5
7	Firma contrato	Amenazas humanas	Informacion Alterada o erronea brindada por el conductor	3	3	3
8	Ingresa a planilla	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al conductor	3	2	2.5
9	Induccion	Amenazas naturales	Modificacion de ficha de documentos del conductor	4	3	3.5
10	entrevista al postulante	Amenazas humanas	Informacion Alterada o erronea del conductor	3	3	3
11	Verificacion de datos referenciales	Amenazas humanas	Modificacion de ficha de documentos del conductor	4	2	3
12	Depuracion de Curriculus	Amenazas humanas	eliminacion por virus, ordenadores fallidos o infomaciones dañadas ya sea Curriculus vitaes.	3	3	3
13	Publicacion de perfil	Amenazas tecnológicas	Informacion Alterada o erronea del conductor	3	2	2.5
14	Puesto nuevo o existente	Amenazas en instalaciones	Informacion Alterada o erronea del conductor	3	3	3

15	Efectua la solicitud según el puesto perfil	Amenazas humanas	Informacion Alterada o erronea del conductor	4	2	3
16	Verifica presupuesto	Amenazas humanas	Informacion Alterada o erronea del conductor	4	3	3.5
17	Solicita pedido de personal	Amenazas tecnológicas	Informacion Alterada o erronea del conductor	3	2	2.5
18	Requerimiento de documentos personales	Amenazas humanas	Informacion Alterada o erronea del conductor	2	1	1.5
19	Rechaza	Amenazas humanas	Informacion Alterada o erronea del conductor	2	1	1.5
20	Windows 10 Pro de RRHH	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	4	2	3
21	Windows 10 Pro de Area Solicitante	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	4	3	3.5
22	Windows 10 Pro Area de Almacen	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	3	2	2.5
23	Windows 10 Pro Area de Contabilidad	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	2	1	1.5

24	Windows 10 Pro del Area de SOMA	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	2	1	1.5
25	Windows Server 2016	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	4	2	3
26	Microsoft Oficce 2016	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	4	3	3.5
27	Eset Antivirus	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	3	2	2.5
28	Active Directory	Amenazas tecnológicas	virus o error de parte del ordenador que brinda esta gestion al Usuario	2	1	1.5
29	Usuario Red RRHH	Amenazas tecnológicas	Perdida de Clave o contraseña facil de cifrar	2	1	1.5
30	Usuario de Red Solicitante	Amenazas tecnológicas	Perdida de Clave o contraseña facil de cifrar	4	2	3
31	Usuario de Red Almacen	Amenazas tecnológicas	Perdida de Clave o contraseña facil de cifrar	4	3	3.5
32	Usuario de Red Contabilidad	Amenazas tecnológicas	Perdida de Clave o contraseña facil de cifrar	3	2	2.5
33	Usuario de Red SOMA	Amenazas tecnológicas	Perdida de Clave o contraseña facil de cifrar	2	1	1.5

34	Correo Corporativo RRHH	Amenazas tecnológicas	Vulnerabilidad ante correos SPAM	2	1	1.5
35	Correo Corporativo Area Silicitante	Amenazas tecnológicas	Vulnerabilidad ante correos SPAM	4	2	3
36	Correo Corporativo Almacen	Amenazas tecnológicas	Vulnerabilidad ante correos SPAM	4	3	3.5
37	Correo Corporativo Contabilidad	Amenazas tecnológicas	Vulnerabilidad ante correos SPAM	3	2	2.5
38	Correo Corporativo SOMA	Amenazas tecnológicas	Vulnerabilidad ante correos SPAM	2	1	1.5

Tabla 22: Análisis de vulnerabilidad

N°	ACTIVOS TI AFECTADOS	ANALISIS DE VULNERABILIDAD				
		CONTROLAMIENTOS PREVENTIVOS	CONTROLAMIENTOS DETECTIVOS	CONTROLAMIENTOS CORRECTIVOS	Clasificación de Vulnerabilidades	Nivel de Vulnerabilidad
1	Listado de Conductor	2	3	1	Control accesos	2
2	Prueba de conduccion	2	3	1	Seguridad de r.r.h.h	2
3	Devolucion de documentos	2	2	1	Control accesos	1.7
4	Evaluacion ruta	3	2	1	Seguridad de r.r.h.h	2
5	Devolucion de documentos	3	2	2	Control accesos	2.3
6	Requerimiento de documentos personales	2	3	3	Seguridad de r.r.h.h	2.7
7	Firma contrato	1	3	2	Seguridad de r.r.h.h	2

8	Ingresa a planilla	1	1	1	Control accesos	1
9	Induccion	3	2	1	Seguridad física y ambiental	2
10	entrevista al postulante	3	2	2	Seguridad de r.r.h.h	2.3
11	Verificacion de datos referenciales	3	1	1	Seguridad de r.r.h.h	1.7
12	Depuracion de Curriculus	3	2	2	Seguridad de r.r.h.h	2.3
13	Publicacion de perfil	3	1	2	Control accesos	2
14	Puesto nuevo o existente	3	2	1	Seguridad de r.r.h.h	2
15	Efectua la solicitud según el puesto perfil	3	1	1	Control accesos	1.7
16	Verifica presupuesto	2	1	1	Control accesos	1.3
17	Solicita pedido de personal	3	1	3	Seguridad de r.r.h.h	2.3

18	Requerimiento de documentos personales	1	1	3	Seguridad de r.r.h.h	1.7
19	Rechaza	3	2	2	Seguridad de r.r.h.h	2.3
20	Windows 10 Pro de RRHH	3	2	1	Administración de las operatividad y conectividad	2
21	Windows 10 Pro de Area Solicitante	3	1	1	Administración de las operatividad y conectividad	1.7
22	Windows 10 Pro Area de Almacen	2	1	1	Administración de las operatividad y conectividad	1.3
23	Windows 10 Pro Area de Contabilidad	3	1	3	Administración de las operatividad y conectividad	2.3
24	Windows 10 Pro del Area de SOMA	1	1	3	Administración de las operatividad y conectividad	1.7
25	Windows Server 2016	3	2	2	Administración de las operatividad y conectividad	2.3
26	Microsoft Oficce 2016	3	2	1	Administración de las operaciones y comunicaciones	2

27	Eset Antivirus	3	1	1	Administración de las operaciones y comunicaciones	1.7
28	Active Directory	2	1	1	Administración de las operaciones y comunicaciones	1.3
29	Usuario Red RRHH	3	1	3	Control de acceso	2.3
30	Usuario de Red Solicitante	1	1	3	Control de acceso	1.7
31	Usuario de Red Almacen	3	2	2	Control de acceso	2.3
32	Usuario de Red Contabilidad	3	2	1	Control de acceso	2
33	Usuario de Red SOMA	3	1	1	Control de acceso	1.7
34	Correo Corporativo RRHH	2	1	1	Control de acceso	1.3
35	Correo Corporativo Area Silicitante	3	1	3	Control de acceso	2.3

36	Correo Corporativo Almacen	1	1	3	Control de acceso	1.7
37	Correo Corporativo Contabilidad	3	2	2	Control de acceso	2.3
38	Correo Corporativo SOMA	1	1	3	Control de acceso	1.7

N°	ACTIVOS TI AFECTADOS	NIVELES	OCURRENCIA

		NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD	PROBABILIDAD	NIVEL
1	Listado de Conductor	3.5	2	2.8	Medio
2	Prueba de conduccion	4.5	2	3.3	Medio
3	Devolucion de documentos	3.5	1.7	2.6	Medio
4	Evaluacion ruta	2	2	2	Medio
5	Devolucion de documentos	3	2.3	2.7	Medio
6	Requerimiento de documentos personales	2.5	2.7	2.6	Medio
7	Firma contrato	3	2	2.5	Medio
8	Ingresa a planilla	2.5	1	1.8	Medio
9	Induccion	3.5	2	2.8	Medio
10	entrevista al postulante	3	2.3	2.7	Medio
11	Verificacion de datos referenciales	3	1.7	2.4	Medio
12	Depuracion de Curriculus	3	2.3	2.7	Medio
13	Publicacion de perfil	2.5	2	2.3	Medio
14	Puesto nuevo o existente	3	2	2.5	Medio
15	Efectua la solicitud según el puesto perfil	3	1.7	2.4	Medio

16	Verifica presupuesto	3.5	1.3	2.4	Medio
17	Solicita pedido de personal	2.5	2.3	2.4	Medio
18	Requerimiento de documentos personales	1.5	1.7	1.6	Medio
19	Rechaza	1.5	2.3	1.9	Medio
20	Windows 10 Pro de RRHH	3	2	2.5	Medio
21	Windows 10 Pro de Area Solicitante	3.5	1.7	2.6	Medio
22	Windows 10 Pro Area de Almacen	2.5	1.3	1.9	Medio
23	Windows 10 Pro Area de Contabilidad	1.5	2.3	1.9	Medio
24	Windows 10 Pro del Area de SOMA	1.5	1.7	1.6	Medio
25	Windows Server 2016	3	2.3	2.7	Medio
26	Microsoft Oficce 2016	3.5	2	2.8	Medio
27	Eset Antivirus	2.5	1.7	2.1	Medio
28	Active Directory	1.5	1.3	1.4	Bajo
29	Usuario Red RRHH	1.5	2.3	1.9	Medio
30	Usuario de Red Solicitante	3	1.7	2.4	Medio
31	Usuario de Red Almacen	3.5	2.3	2.9	Medio
32	Usuario de Red Contabilidad	2.5	2	2.3	Medio
33	Usuario de Red SOMA	1.5	1.7	1.6	Medio
34	Correo Corporativo RRHH	1.5	1.3	1.4	Bajo
35	Correo Corporativo Area Silicitante	3	2.3	2.7	Medio

36	Correo Corporativo Almacen	3.5	1.7	2.6	Medio
37	Correo Corporativo Contabilidad	2.5	2.3	2.4	Medio
38	Correo Corporativo SOMA	1.5	1.7	1.6	Medio

3.6.- FASE 5: Identificación de Alarmas. -

Tabla 23: Identificación de Alarmas

ANALISIS DE NIVEL DE ALARMA											
N°	ACTIVOS DE TI AFECTADOS	Amenaza	IMPACTO			Valor de Activo	Probabilidad de ocurrencia	Nivel de impacto	Valoracion de Alarma	
			Impacto económico para la empresa	Impacto Operacional de la empresa					Nivel de exposición al Alarma	Nivel de Alarma
1	Listado de Conductor	Amenazas humanas	4	4	4	4	2.8	4	3.6	Alto
2	Prueba de conduccion	Amenazas humanas	4	4	4	4	3.3	4	3.8	Alto
3	Devolucion de documentos	Amenazas tecnológicas	5	4	4.5	4.3	2.6	4.5	3.8	Alto
4	Evaluacion ruta	Amenazas humanas	3	5	4	3.3	2	4	3.1	Medio
5	Devolucion de documentos	Amenazas humanas	1	2	1.5	3	2.7	1.5	2.4	Medio
6	Requerimiento de documentos personales	Amenazas humanas	3	1	2	4.3	2.6	2	3.0	Medio
7	Firma contrato	Amenazas humanas	5	3	4	4.3	2.7	4	3.7	Alto

8	Ingresa a planilla	Amenazas tecnológicas	4	4	4	4	1.9	4	3.3	Medio
9	Induccion	Amenazas naturales	4	5	4.5	3	2.9	4.5	3.5	Medio
10	entrevista al postulante	Amenazas humanas	2	4	3	3	2.9	3	3.0	Medio
11	Verificacion de datos referenciales	Amenazas humanas	1	3	2	3	2.5	2	2.5	Medio
12	Depuracion de Curriculus	Amenazas humanas	4	2	3	3.3	2.9	3	3.1	Medio
13	Publicacion de perfil	Amenazas tecnológicas	2	3	2.5	3	2.6	2.5	2.7	Medio
14	Puesto nuevo o existente	Amenazas en instalaciones	4	2	3	3	2.9	3	3.0	Medio
15	Efectua la solicitud según el puesto perfil	Amenazas humanas	3	5	4	4	3.5	4	3.8	Alto
16	Verifica presupuesto	Amenazas humanas	2	4	3	3	2.8	3	2.9	Medio
17	Solicita pedido de personal	Amenazas tecnológicas	3	3	3	4	3.4	3	3.5	Medio

18	Requerimiento de documentos personales	Amenazas humanas	2	2	2	3	2.1	2	2.4	Medio
19	Rechaza	Amenazas humanas	5	3	4	3	2.6	4	3.2	Medio
20	Windows 10 Pro de RRHH	Amenazas tecnológicas	1	5	3	0	2.7	3	1.9	Medio
21	Windows 10 Pro de Area Solicitante	Amenazas tecnológicas	5	4	4.5	3.7	2.8	4.5	3.7	Alto
22	Windows 10 Pro Area de Almacen	Amenazas tecnológicas	1	3	2	3.7	2.1	2	2.6	Medio
23	Windows 10 Pro Area de Contabilidad	Amenazas tecnológicas	1	2	1.5	3.7	1.4	1.5	2.2	Medio
24	Windows 10 Pro del Area de SOMA	Amenazas tecnológicas	2	3	2.5	3.7	1.9	2.5	2.7	Medio
25	Windows Server 2016	Amenazas tecnológicas	1	2	1.5	3.7	2.7	1.5	2.6	Medio
26	Microsoft Oficce 2016	Amenazas tecnológicas	3	4	3.5	4	2.8	3.5	3.4	Medio
27	Eset Antivirus	Amenazas tecnológicas	5	5	5	3.3	2.1	5	3.5	Medio

28	Active Directory	Amenazas tecnológicas	5	5	5	3.7	1.4	5	3.4	Medio
29	Usuario Red RRHH	Amenazas tecnológicas	5	5	5	3.7	1.9	5	3.5	Alto
30	Usuario de Red Solicitante	Amenazas tecnológicas	1	1	1	3.7	2.7	1	2.5	Medio
31	Usuario de Red Almacen	Amenazas tecnológicas	1	5	3	3.7	2.8	3	3.2	Medio
32	Usuario de Red Contabilidad	Amenazas tecnológicas	5	4	4.5	3.7	2.1	4.5	3.4	Medio
33	Usuario de Red SOMA	Amenazas tecnológicas	1	3	2	3.7	1.4	2	2.4	Medio
34	Correo Corporativo RRHH	Amenazas tecnológicas	1	2	1.5	3.7	1.9	1.5	2.4	Medio
35	Correo Corporativo Area Silicitante	Amenazas tecnológicas	2	3	2.5	3.7	2.7	2.5	3.0	Medio
36	Correo Corporativo Almacen	Amenazas tecnológicas	1	2	1.5	3.7	2.6	1.5	2.6	Medio
37	Correo Corporativo Contabilidad	Amenazas tecnológicas	3	4	3.5	3.7	2.4	3.5	3.2	Medio

38	Correo Corporativo SOMA	Amenazas tecnológicas	5	5	5	3.7	1.6	5	3.4	Medio

3.7.-FASE 6: Análisis de Alarmas

De acuerdo a los cuadros obtenidos en la identificación de alarmas, luego de brindar un valor a cada ocurrencia, se procede a evaluar los alarmas que tiene valor Medio, Alto y Muy Alto por ser de mayor consideración y que generan impacto en la empresa. No se considera a los que hayan obtenido en el proceso "Nivel de Alarma" como resultado Bajo debido a que sus características preceden de valores bajos esto muestra que no genera impacto en la organización.

Tabla 24: Análisis de nivel de alarma

ANALISIS DE NIVEL DE ALARMA			
N°	ACTIVOS DE TI AFECTADOS	Valoracion de Alarma	
		Nivel de exposición al Alarma	Nivel de Alarma
1	Listado de Conductor	3.6	Alto
2	Prueba de conduccion	3.8	Alto
3	Devolucion de documentos	3.8	Alto
4	Evaluacion ruta	3.1	Medio
5	Devolucion de documentos	2.4	Medio
6	Requerimiento de documentos personales	3.0	Medio
7	Firma contrato	3.7	Alto
8	Ingresa a planilla	3.3	Medio
9	Induccion	3.5	Medio
10	entrevista al postulante	3.0	Medio
11	Verificacion de datos referenciales	2.5	Medio
12	Depuracion de Curriculum	3.1	Medio
13	Publicacion de perfil	2.7	Medio
14	Puesto nuevo o existente	3.0	Medio
15	Efectua la solicitud según el puesto perfil	3.8	Alto
16	Verifica presupuesto	2.9	Medio
17	Solicita pedido de personal	3.5	Medio
18	Requerimiento de documentos personales	2.4	Medio
19	Rechaza	3.2	Medio
20	Windows 10 Pro de RRHH	1.9	Medio
21	Windows 10 Pro de Area Solicitante	3.7	Alto
22	Windows 10 Pro Area de Almacen	2.6	Medio
23	Windows 10 Pro Area de Contabilidad	2.2	Medio
24	Windows 10 Pro del Area de SOMA	2.7	Medio
25	Windows Server 2016	2.6	Medio
26	Microsoft Oficce 2016	3.4	Medio
27	Eset Antivirus	3.5	Medio
28	Active Directory	3.4	Medio
29	Usuario Red RRHH	3.5	Alto
30	Usuario de Red Solicitante	2.5	Medio

31	Usuario de Red Almacen	3.2	**Medio**
32	Usuario de Red Contabilidad	3.4	**Medio**
33	Usuario de Red SOMA	2.4	**Medio**
34	Correo Corporativo RRHH	2.4	**Medio**
35	Correo Corporativo Area Silicitante	3.0	**Medio**
36	Correo Corporativo Almacen	2.6	**Medio**
37	Correo Corporativo Contabilidad	3.2	**Medio**
38	Correo Corporativo SOMA	3.4	**Medio**

3.8.- FASE 7: Respuesta a Alarmas

Tabla 25: Respuesta a Alarmas(desde aquia)

N°	ACTIVOS DE TI AFECTADOS	AMENAZAS	TIPO DE TRATAMIENTO	CONTROLAMIENTOS DE PROTECCIÓN PROPUESTOS	DESCRIPCIÓN / OBSERVACIONES	CONTROL A IMPLEMENTAR	ALARMA RESIDUAL	ALARMA SECUNDARIO	CONTROL MEJORADO A IMPLEMENTAR
1	Listado de Personal Administrativo y Conductor	Amenazas humanas	Reducir	A.11.1.2. Las áreas correctamente de controlamientos apropiados	Prevencion, proteccion y resguardacion todo lo que es considerado como susceptible de robo, perdida o daño; esta restriccion puede ser aplicada a sistemas de informaciones .	Directrices de control de acceso a directorios	No se llegó a guardar por completo, se dañó el archivo	Usuarios no pueden abrir el archivo	Verificación del archivo después de guardar, realizar backups del archivo, gestionar los permisos de los usuarios
2	Prueba de conducción	Amenazas humanas	Aceptar	A.8.1.4. La privacidad y la ser aseguradas tal como se requiere en la	La protección de datos es el proceso de proteger la información importante de la	Almacenar los documentos en gavetas distribuidas por secciones	Pérdida por robo de la gaveta y documentos importantes	Pérdida y/o extravío de la llave de gaveta	Realizar una copia digitalización, guardarlo en el servidor y

				legislación y regulación relevante donde sea aplicable	corrupción y/o pérdida. El término protección de datos se utiliza para el respaldo operativo de datos y la recuperación de desastres.				generar backups de los archivos, respaldo con permisos de seguridad, cada uno con su respectivo nombre para su mejor control
6	Requerimiento de documentos personales	Amenazas humanas	Aceptar	A.11.1.4. Protección física contra desastres naturales, ataques maliciosos, deben ser diseñada y aplicada. A.8.3.3 Tienen informaciones deberian ser cuidados contra accesados no autorizados, la averìa en su envio	Se trata de una estrategia planificada y especializada para asegurar que los datos y toda la información se encuentren disponibles a largo plazo sin sufrir alteración y pérdidas.	Realizar el requerimiento de los documentos con sus respectivos nombres y numero de documentos,	No tener los documentos requeridos, especificados en el aviso	Documentos no se distinguen las letras(borrosos)	Filtrar los documentos requeridos especialmente para el área solicitante, con documentos legibles en buen estado

7	Firma contrato	Amenazas humanas	Aceptar	A.8.3.3 Tienen informaciones deberian ser cuidados contra accesados no autorizados, la averìa en su envio	Los activos de informaciones tienen que estar agrupados por sensibilidad y criticidad en información que cumplen con objetivo cómo ha de ser tratado y cuidada la información.	realizar una copia de los documentos firmados en gavetas seleccionadas para su uso	documentos no encontrados,	documentos dañados	implementar copias digitalizadas, guardadas en un disco externo protegido con respaldos de backup y guardarlos con su respectivo nombre y documento para su mejor control
17	Solicita pedido de personal	Amenazas tecnológicas	Aceptar	A.8.3.3 Tienen informaciones deberian ser cuidados contra accesados no autorizados, la averìa en su envio	Los activos de informaciones tienen que estar agrupados por sensibilidad y criticidad en información que cumplen con objetivo cómo ha de ser tratado y cuidada la información.	Implementar un sistema de control de pedido de personal, un formato establecido para el requerimiento y/o correo emitido al área de recursos humanos.	No haber escrito bien los requerimiento de pedido de personal	Pérdida de conexión, correos no llegan al destino	Implementar un mejor control verificando la escritura, ortografía, y verificando la conexión de internet.

21	Windows 10 PRO área Solicitante	Amenazas tecnológicas	Reducir	A.8.3.3 Tienen informaciones deberian ser cuidados contra accesados no autorizados, la averìa en su envio	Los activos de informaciones tienen que estar agrupados por sensibilidad y criticidad en información que cumplen con objetivo cómo ha de ser tratado y cuidada la información.	Identificar y descartar softwares maliciosos	No contar con software de protección	Sistema operativo dañado	Implementar y instalar software que protegan los sistemas operativos

CAPITULO 4

Con el proyecto de investigación, JPLOGÍSTICAS.A.C.. contará con conocimiento de los activos importantes, los alarmas y amenazas que estos pueden tener. Con esto se busca que se tenga mayor seguridad sobre estos activos de mayores alarmas.

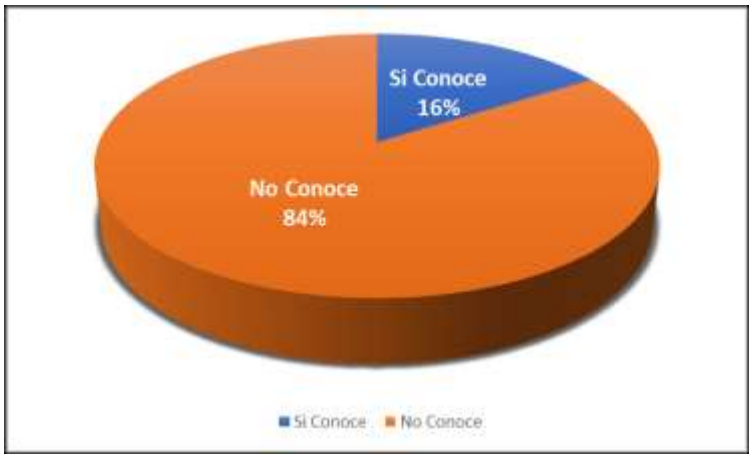
Resultado 1: Inventariar y clasificar los Activos del Proceso de "Selección e Inducción del Personas Administrativas y Conductor"

Tipo Activo	Valoración Alta	Valoración Media	Valoración Baja
Activos de informaciones	8	11	0
Activos de Software	18	1	0
Activos Hardware	0	0	12
Personal	0	0	6

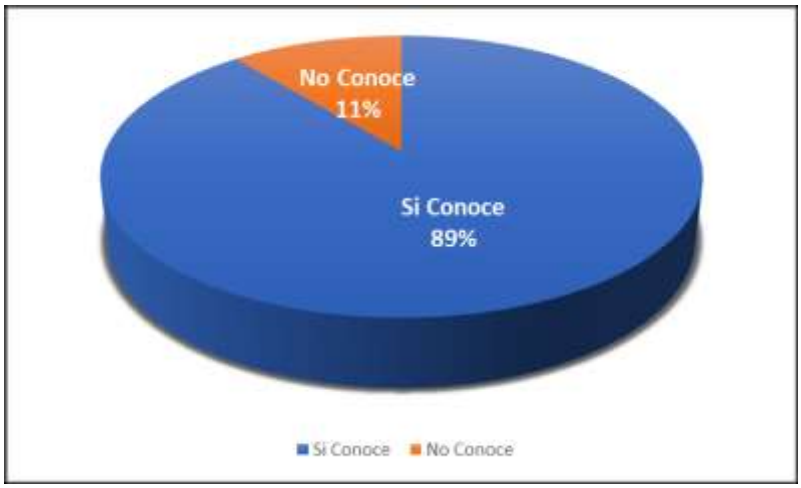
Ver Anexo 1: Listado de Activos

- De acuerdo al primer objetivo para obtener la satisfacción se realizó encuestas: El grado de satisfacción fue el óptimo.

Recuento de P1 ¿Conoce Ud. Cuáles son los Activos en Procesos de "Selección e Inducción en Personal Administrativo y Conductor" y como están clasificados?



Recuento de P2 ¿Actualmente con el Inventario y Clasificación de Activos del Proceso de "Selección e Inducción en Personal Administrativo y Conductor", Ud. conoce los activos?



Resultado 2: Identificar y Clasificar los Alarmas para el Proceso de "Selección e Inducción del Personal Administrativo y Conductor".

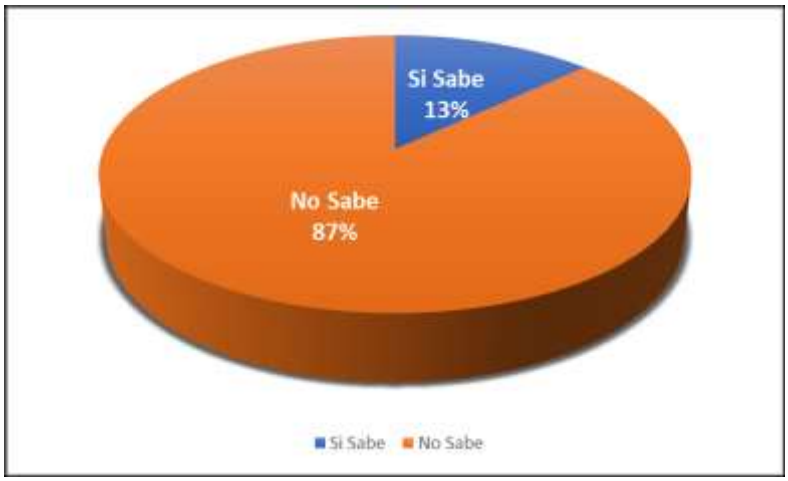
Tipo Activo	Valoración Baja	Valoración Media	Valoración Alta	Valoración Muy Alta
Activos de informaciones	0	7	9	3
Activos de Software	0	0	0	0

Activos Hardware	0	0	0	0
Personal	0	0	0	0

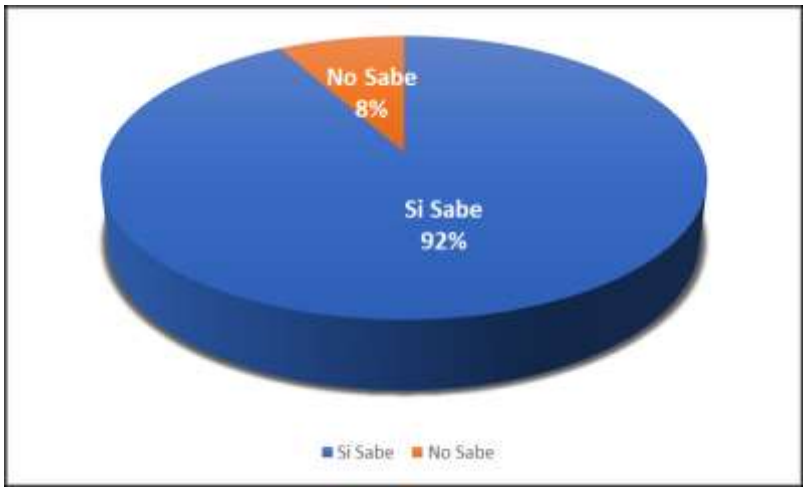
Ver Anexo 2: Análisis de nivel de alarma

- De acuerdo al segundo objetivo para obtener la satisfacción se realizó encuestas: El grado de satisfacción fue el óptimo.

Recuento de P1 ¿Sabia Ud. Cuáles son los alarmas y su clasificación de los alarmas en el Proceso de "Selección e Inducción del Personal Administrativo y Conductor"



Recuento de P2 ¿Actualmente con la identificación y clasificación de los alarmas en el Procesos de "Selección e Inducción en Personal Administrativo y Conductor" Ud. sabe identificar los alarmas?



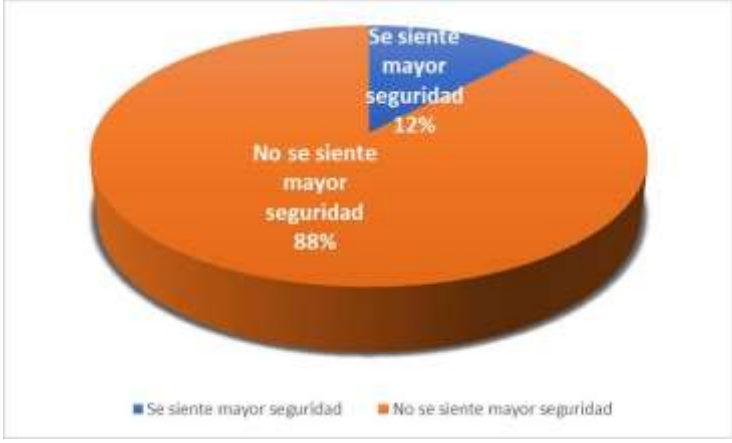
Resultado 3: Establecer Controlamientos para el Mitigacionamiento de alarmas identificados en el Procesos de Inducción al Personal Administrativo y Conductor.

Anexo 3: Controlamientos para el tratamiento para los alarmas identificados

- De acuerdo al tercer objetivo para obtener la satisfacción se realizó encuestas:

El grado de satisfacción fue el óptimo

Recuento de P1 ¿Los Activos del proceso de "Selección e Inducción del Personal Administrativo y Conductor", que tiene mayor alarma y que no tienen controlamientos, ¿siente Ud. que su activo es más seguro?



Recuento de P2: ¿Después de aplicar los Controlamientos a los Activos en el Proceso de "¿Selección e Inducción del Personal Administrativo y Conductor" que tienen mayor alarma, Ud. se siente más seguro?

ACTA DE CONFORMIDAD

En la siguiente acta de hace mención a la conformidad satisfactoria de parte del interesado principal de la implementación de una metodología para gestionar los alarmas.

JP Logística	**ACTA DE CONFORMIDAD**
Nro. ORDEN DE SERVICIO	SGI-01
CONTRATISTA	Yoel Lopez Leiva
Nro. RUC	20518404963
DESCRIPCION DEL SERVICIO	Implementar una Metodología para Gestionar los Alarmas en el Proceso de Selección e Inducción del Personal Administrativo y Conductor basada en el PMBOK y MAGERI.T. para la empresa JPLOGÍSTICAS.A.C..
FECHA DE INICIO	02/02/2018
FECHA DE TERMINO	14/06/2018
USUARIO	Juan Pérez Matías

Que se ha recibido a satisfacción de JP LOGISTICA SAC, los servicios brindados por el contratista, servicios que corresponden al 100% suscrita. Con todo ello se ha logrado:

- Inventariar y clasificar los Activos del Procesos en Selección e Inducción del Personal Administrativo y Conductor.
- Identificar y Clasificar los Alarmas para el Procesos en Selección e Inducción del Personal Administrativo y Conductor.
- Establecer Controlamientos para el Mitigacionamiento de alarmas identificados en el Proceso de Selección e Inducción del Personal Administrativo y Conductor.

Cuadro de Costos y Presupuestos

Tabla 28: Costos y Presupuestos

Tipo	Recursos	Dedicatoria	Horas Dedicadas	Costo x Hora	Total (S/)
Equipos	Laptop	Tiempo completo			3,000.00
	Computadoras	Para trabajos de oficina			1,800.00
	Sillas	Para trabajos de oficina			300.00
	escritorio	Para trabajos de oficina			600.00
				Sub Total	5,700.00
Licencia	Antivirus	Análisis			200.00
	Office	Análisis			350.00
	Windows	Análisis			600.00
				Sub Total	1,150.00
Personas	especialista en TI	Asistente de proyecto	30	S/20.00	600.00
	Jefe de proyecto	Tiempo completo	1400	S/17.00	23,800.00
	Asistente	Tiempo completo	1500	S/11.00	16,500.00
	Seguridad de TI	Análisis	100	S/30.00	3,000.00
				Sub Total	43,900.00
Varios	Gastos varios				5,000.00
					55,750.00

Anexo 1: Listado de Activos

CLASIFICACIÓN DE ACTIVOS DE TI									
	DATOS			NIVEL DE PILARES DE SI			ACTIVOS DE TI		
ACTIVO	CATEGORIA	CLASIFICACIÓN	FUNCIONALIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DE ACTIVO	NIVEL DE APRECIACION	
			ACTIVOS DE INFORMACIONES						
Listado de Personal Administrativo y Conductor	Información escrita	Restringida	El que será evaluado y el profesional en dicha especialidad	4	4	4	**4**	**Alto**	

Prueba de conducción	Información escrita	Interno	Esta evaluación considera las capacidades de visión y orientación auditiva, la agudeza visual y campimetría, los tiempos de reacción y recuperación al encandilamiento, la capacidad de coordinación de aceleración y frenado.	4	4	4	**4**	**Alto**
Devolución de documentos	Información escrita	Interno	Prueba fallida sobre el conductor o postulante a este puesto.	4	4	5	**4.3**	**Alto**
Evaluación ruta	Información escrita	Interno	Prueba de ruta largas y cortas, tiempos de reacción del conductor.	3	3	4	**3.3**	**Medio**
Devolución de documentos	Información escrita	Interno	Prueba fallida sobre el conductor o postulante a este puesto.	3	4	2	**3**	**Medio**
Requerimiento de documentos personales	Información escrita	Interno	Esta gestión requiere de los documentos personales de dicho conductor dependiendo si aprobó o no la funcionalidad de prueba de conducción.	4	4	5	**4.3**	**Alto**
Firma contrato	Información escrita	Interno	El contrato es acuerdo entre empresa y trabajador legalmente, y que tiene como fin brindar seguridad y protección jurídica a cada una, pues establece los términos y condiciones de la relación laboral, así como los derechos y obligaciones de ambas.	5	5	3	**4.3**	**Alto**

Ingresa a planilla	Información escrita	Interno	Ingresar a planilla de pago de una compañía , y los demás beneficios que se pagan.	5	5	2	**4**	**Alto**
Inducción	Información escrita	Interno	La inducción es el proceso en el conocimiento el cual consiste en analizar observando, situaciones particulares para conclusión.	2	4	3	**3**	**Medio**
entrevista al postulante	Información hablada	Interno	Es una entevista de dos o más personas para tratar algún asunto, generalmente profesional o de negocios con el formato de preguntas predeterminado para cada área.	2	4	3	**3**	**Medio**
Verificación de datos referenciales	Información escrita	Interno	Verificación de datos personales de dicho conductor o postulante. Es primordial para confirmar la veracidad de las referencias o por el contrario prescindir de un candidato por no haber sido del todo sincero, verificación de documentos.	2	4	3	**3**	**Medio**

Depuración de Currículos	Información electrónica	Interno	Depuración y eliminación de CV que ya no están a la disposición o que ya no cumplan con los requisitos del puesto.	3	4	3	**3.3**	**Medio**
Publicación de perfil	Información electrónica	Público	Publicación del perfil del puesto al que se están postulando, mediante una publicación vía internet o correo (corporativo, Gmail, etc.)	2	3	4	**3**	**Medio**
Puesto nuevo o existente	Información electrónica	Interno	Verificación del puesto si existe o no mediante un correo preguntando al administrador del puesto existente en caso contrario informaran que el puesto no existe.	3	3	3	**3**	**Medio**
Efectúa la solicitud según el puesto perfil	Información escrita	Interno	Efectúa y verifica el personal según como requiere el área solicitante, mediante correos electrónicos o documentos (CV).	4	4	4	**4**	**Alto**
Verifica presupuesto	Información electrónica	Interno	El área de contabilidad hace la verificación si cumplen con los requisitos para dicho beneficio del conductor o colaborador.	2	3	4	**3**	**Medio**
Solicita pedido de personal	Información electrónica	Interno	Una solicitud es carta contacto envíada a una empresa en la que se quiere trabajar. La persona debe explicar de manera formal, cuál es el motivo de su contacto y detallar su experiencia, aptitudes, etc. mediante correo electrónico o presencial.	4	4	4	**4**	**Alto**

Requerimiento de documentos personales	Información electrónica	Interno	Una vez pasada la evaluación y aceptada la oferta se pasa al siguiente requerir los documentos de dicho postulante.	2	3	4	**3**	**Medio**
Rechaza	Información electrónica	Público	Prueba fallida sobre el conductor o postulante a este puesto.	2	4	3	**3**	**Medio**
			ACTIVOS DE SOFTWARE					
WINDOWS 10 PRO 64 BIT	Información electrónica	Interno	Sistema operativo, plataforma por el cual el usuario interactúa, por el cual genera archivos con contienen información valiosa para la empresa	1	2	1	**1.3**	**Bajo**
WINDOWS SERVER 2012 R2	Información electrónica	Interno	Sistema operativo, plataforma por el cual el usuario interactúa, con el que gestiona y distribuye la información valiosa de empresa a los usuarios, genera archivos con contienen información valiosa para la empresa	1	1	2	**1.3**	**Bajo**
OFFICE 2016	Información electrónica	Interno	Programa por el cual se generan archivos, cuadros, presentaciones, documentos para la empresa que contienen información valiosa.	2	1	1	**1.3**	**Bajo**
ESET ANTIVIRUS	Información electrónica	Interno	Programa creado especialmente para poder evitar infectar nuestro equipo PC de virus, malware, troyanos, etc., proteger información valiosa para la empresa	1	1	1	**1**	**Bajo**
			ACTIVOS HARDWARE					

SERVIDOR LENOVO THINKSERVER TS 150	Información electrónica	Restringida	Equipo especial para la funcionabilidad de servidores para labores pesadas, de horas de trabajo continuas.	1	1	2	**1.3**	**Bajo**
EQUIPO INTEL COREI7 RAM8GB	Información electrónica	Público	Equipo especial para la funcionabilidad de sistemas operativos (Windows 10), para la labor del usuario.	2	1	1	**1.3**	**Bajo**
SWITCH TPLINK DE 24 PUERTOS	Información electrónica	Restringida	Dispositivo para la distribución de cableado/conectividad de cada equipo (PC), distribución de la información	1	2	1	**1.3**	**Bajo**
SWITCH TPLINK DE 16 PUERTOS	Información electrónica	Restringida	Dispositivo para la distribución de cableado/conectividad de cada equipo (PC), distribución de la información	2	1	1	**1.3**	**Bajo**
			PERSONAL					
PSICÓLOGO	Información hablada	Interno	Personal especializado para el filtro de la selección de personal requerido para el área solicitante.	2	1	1	**1.3**	**Bajo**

Anexo 2: Análisis de nivel de alarma

ANALISIS DE NIVEL DE ALARMA									
N°	ACTIVOS DE TI AFECTADOS	IMPACTO			Valor de Activo	Probabilidad de Ocurrencia	Nivel de impacto	ALARMA INHERENTE	
		Impacto Económico	Impacto Operacional	Nivel de impacto				Nivel de exposición al Alarma	Nivel de Alarma
1	Listado del Personal Administrativo y Conductor.doc	4	4	4	4	3.4	4	13.6	Alto
2	Prueba de conduccion.doc	4	4	4	4	3.6	4	14.4	Alto
3	Devolución de documentos.doc	5	4	4.5	4.3	3.6	4.5	16.2	Muy Alto
4	Evaluación ruta.doc	3	5	4	3.3	3.6	4	14.4	Alto
5	Devolución de documentos.pdf	1	2	1.5	3	3.7	1.5	5.55	Medio
6	Requerimiento de documentos personales.pdf	3	1	2	4.3	3.9	2	7.8	Medio
7	Firma contrato.doc	5	3	4	4.3	3.4	4	13.6	Alto
8	Ingresa a planilla.doc	4	4	4	4	3.3	4	13.2	Alto
9	Induccion.pdf	4	5	4.5	3	3.3	4.5	14.85	Alto

10	entrevista al postulante.pdf	2	4	3	3	3.4	3	10.2	Alto
11	Verificación de datos referenciales.pdf	1	3	2	3	3	2	6	Medio
12	Depuración de Curriculus.doc	4	2	3	3.3	3.2	3	9.6	Alto
13	Publicación de perfil.doc	2	3	2.5	3	3.3	2.5	8.25	Medio
14	Puesto nuevo o existente.doc	4	2	3	3	2.9	3	8.7	Medio
15	Efectúa la solicitud según el puesto perfil.doc	3	5	4	4	4.4	4	17.6	Muy Alto
16	Verifica presupuesto.doc	2	4	3	3	2.9	3	8.7	Medio
17	Solicita pedido de personal.pdf	3	3	3	4	3.4	3	10.2	Alto
18	Requerimiento de documentos personales.pdf	2	2	2	3	3.6	2	7.2	Medio
19	Rechaza.doc	5	3	4	3	4.1	4	16.4	Muy Alto

Anexo 3: Controlamientos para el mitigacionamiento de alarmas identificados

EVALUACIÓN DEL ALARMA INHERENTE										
°N	ACTIVOS DE TI AFECTADOS	Amenazas	Tipo de tratamiento	Controlamientos ódeproteccin propuestos	óDescripcin / Obeservaciones	Control a implementar	Alarma Residual	Alarma Secundario	Control mejorado a implementar	Cumplimiento del Control - ISO/NTP/IEC 27001
1	Listado de Conductor	Amenazas humanas	Reducir	A.11.1.2.Las areas seguras deben ser cuidadas por medio de controlamientos apropiados	Los activos de informaciones tienen que estar clasificados .	documentos en files y/o en una gabeta asegurada con llave proteccion contra robo y deterioro por el ambiente	deterioro por humedad	extraviar la llave y no poder tener acceso a ello	copia de llave y copia de documente como respaldo	Seguridad física y del entorno
2	Prueba de conduccion	Amenazas humanas	Aceptar	A.8.1.4.La privacidad de datos personales deben ser aseguradas segun la legislacion relevante donde sera aplicada	La protección de datos es el proceso de proteger la información. El término protección de datos se utiliza respaldo operativo de datos y la recuperación .	documentos en files y/o en una gabeta asegurada con llave proteccion contra robo y deterioro por el ambiente	deterioro por humedad	extraviar la llave y no poder tener acceso a ello	copia de llave y copia de documente como respaldo	Directrices de seguridad

3	Devolucion de documentos	Amenazas tecnológicas	Aceptar	A.11.1.2.Las areas seguras deben ser protegidas por medio de controlamientos apropiados	Prevenir, proteger y resguardar todo lo que es considerado como susceptible de robo, perdida o daño; esta excepción puede ser aplicada a los sistemas de informaciones en general ya se que pertenezcan a grupo o empresa u organización.	se implementa un contrl de devolucion de documentos con la firma y el nombre del usuario asi confirmando su devolucion de dicho documento	olvido de firmar el documento de control y perdida de informacion	Docuementos faltantes al finalizar la revision	Implementacion de Foliado y Etiquetado	Directrices de seguridad
7	Firma contrato	Amenazas humanas	Aceptar	A.8.3.3 Tienen informaciones deberian ser cuidados contra accesados no autorizados, la averìa en su envio	Los activos de informaciones tienen que estar clasificados según la sensibilidad y criticidad de la información que contienen o que cumplen con el objetivo de señalar cómo ha de ser trata y	realizar una copia de los documentos firmados en gavetas seleccionadas para su uso	Documentos no encontrados	Documentos Dañados	implementar copias digitalizadas, guardadas en un disco externo protegido con respaldos de backup y guardarlos con su respectivo nombre y documento	Seguridad de los recursos humanos

					protegida la información.				para su mejor control	
15	Efectua la solicitud según el puesto perfil	Amenazas humanas	Aceptar	A.8.3.3 Tienen informaciones deberian ser cuidados contra accesados no autorizados, la averìa en su envio	Segun criticidad cumplen con la meta de senalar como se debe tartar.	Implementar un procedimiento y formato para llenado de Perfil	No detallado del perfil y no cumplan con el perfil asignado	Formato no ubicado	Implementacion de politicas de seguridad y formatos para guardarlos en zonas seguras	Seguridad de los recursos humanos
21	Windows 10 Pro de Area Solicitante	Amenazas tecnológicas	Reducir	A.8.3.3 Tienen informaciones deberian ser cuidados contra accesados no autorizados, la averìa en su envio	Prevenir, proteger y resguardar perdida o daño; esta excepción puede ser aplicada a los sistemas de informaciones en general ya se que pertenezcan a grupo o empresa.	Implementar procedimientos de limpieza de software	Lentitud por Descargas de actualizacion y parches de seguridad	Software incompatible con aplicativos de la empresa	Implementacion de Politicas y procedmientos para mantenimiento de software	Politicas de Seguridad

29	Usuario Red RRHH	Amenazas tecnológicas	Reducir	A.8.3.3 Tienen informaciones deberian ser cuidados contra accesados no autorizados, la averìa en su envio	Prevenir, proteger y resguardar perdida o daño; esta excepción puede ser aplicada a los sistemas de informaciones en general ya se que pertenezcan a grupo o empresa.	Implementacion de politicas de usuario en el servidor	Restricciones en aplicativos que no podrian funcionar	Restriccion de funcionamiento de algunos aplicativos	Implementacion de politicas y procedimientos para usuarios de red	Politicas de Seguridad

CONCLUSIONES

El presente trabajo investigativo en Ingeniería de Sistemas e Informática, se puede concluir lo siguiente:

1. Se inventarió y se realizó la clasificación de los activos del proceso de evaluación del personal, vía la definición del alcance que tendría la implementación de la metodología PMBOK y MAGERI.T. para el análisis y gestionamiento en alarmas de la seguridad en las informaciones en el proceso de inducción del personal en la Empresa JPLogísticaS.A.C., fue clave y fundamental para viabilizar este proyecto, ya que la empresa no contaba con el estudio y la experiencia para el análisis de alarmas de un sistematización de gestionamiento de seguridad en las informaciones y el tener explícitamente definido el alcance.

2. Se realizó el análisis de la gestionamiento en alarmas para el proceso de evaluación del personal vía el apoyo de la alta gerencia para inventariar y clasificar los activos del proceso de evaluación de personal y transportista en la Empresa JPLogísticaS.A.C. para el Diseñamiento de los procesos de implementación fue imprescindible, debido a que fue necesaria su participación para ayudar a sensibilizar a los jefes de área y de las actividades que operativizan, con la finalidad de participar de las entrevistas para el levantamiento de informaciones de inventariar y clasificar los activos, que ayudó a que comprendieran que los alarmas de un sistematización de gestionamiento de seguridaden las informaciones no solo busca proteger la información digital, sino de forma integral toda la información crítica del negocio independientemente del medio que la abarca y almacena. .

3. Se estableció controlamientos vía el tratamiento de alarmas informáticos en el proceso de evaluación de personal mediante la implementación de la metodología PMBOK y MAGERI.T. se ha establecido controlamientos para el mitigacionamiento de alarmas informáticos identificados en el proceso de evaluación de personal y transportista en la Empresa JPLogísticaS.A.C.., lo cual permitirá que la gestión de seguridad en las informaciones, asociados a la confidencialidad, integridad y disponibilidad se minimice para obtener óptimos resultados visibles y lograr el mejoramiento continuo de los controlamientos implementados.

RECOMENDACIONES

1. Una recomendación sería que a la Gerencia de la Empresa JPLogísticaS.A.C., la implementación de la metodología PMBOK y MAGERI.T. para el análisis y gestionamiento en alarmas de la seguridad en las informaciones en el proceso de inducción del personal, mediante la adquisición de los servicios de una consultora que pueda guiar el Diseñamiento y la implementación efectiva con estándares y normas vigentes en el Perú.

2. Una recomendación sería empoderar de los mecanismos que permitan a la Gerencia inventariar y clasificar los activos del proceso de evaluación de personal y transportista en JPLogísticaS.A.C.., los activos de informaciones, con la finalidad del levantamiento de informaciones sobre las alarmas de un sistema de gestión de seguridad que no han sido tomados en cuenta, para cubrir todos los escenarios a los que está expuesto la organización.

3. Se recomienda implementar los controlamientos para el mitigacionamiento de alarmas informáticos identificados en el proceso de evaluación de personal y transportista en la Empresa JPLogísticaS.A.C.., para que el futuro no represente una inversión financiera para la organización; si no establecer medidas que garantizan la seguridad de los activos y aseguran la continuidad del negocio frente a los riegos y amenazas de la seguridad de informaciones.

REFERENCIA BIBLIOGRAFICA

Aguirre, D. A. (2014). *Proyecto de Diseñamiento de un sistematización de gestionamiento de seguridadde informaciones para SERPOST Perú S.A.* PUCP.

Angarita, J. A. y Bautista, C. L. (2014*). Proyecto de Diseñamiento de un sistema de gestión de seguridad en las informaciones ISO 27002 para el municipio de Floridablanca y plan de accionar para su implementación basado en Pmbok*. Universidad Industrial de Santander, Bucamaranga – Colombia.

Alexander, A. (2005). *Diseñamiento de un Sistematización de gestionamiento de seguridadde informaciones. Óptica ISO 27001:2005*. Alfaomega Colombiana S.A., Colombia.

Areitio, J.B. (2008). Seguridad en las informaciones. Madrid: Paraninfo.

AZ/NZS 4360, (1999). Administración de Alarmas, Estándar Australiano. Australia - Nuevazelandia.

Bernal, E. R. (2017). Propuesta de planeamiento en alarmas y gestión ética para departamento de tecnologías en Educacion. Universidad de Cuenca, Ecuador.

Conde, O., Núñez, E. y Álvarez, J. (2008). *Manual en Proyectos de Inversión en el Sector Público*. Editora y Distribuidora Real S.R.L. Lima – Perú.

Craig, L. (2003). Agile & Iterative Develoment: A Manager´s Guide, Ed. Addison-Wesler Cruz, M. A. y Fukusaki, S. (2017). *Diseñamiento e implementación de un sistematización de gestionamiento de seguridaden las informaciones para proteger los activos de informaciones en Clínica MED-CAM Perú SA.*. Universidad de San Martín de Porres, Lima – Perú.

Espinoza, R. (2015). *Análisis y Diseñamiento de un Sistematización de gestionamiento de seguridad de informaciones basado en la norma ISO/NTP/IEC 27001:2005 en empresa de producción y comercialización en productos de consumo*. Lima, Perú. PUCP.

Fernández, C., Medina, T., Moya, N. y Plattini, D. (2002). Acceso a información pública y gobierno digital: evaluación de sitios web de principales ayuntamientos andaluces. Universidad de Granada.

García, S. C. (2018). *Modelo en seguridad en las informaciones para incrementar en la gestión de unidades ambientales en Lambayeque*. Universidad Católica Santo Toribio Mogrovejo.

Gordillo, A. C. (2017). *Sistematización de gestionamiento de seguridaden las informaciones en ENELNORTE prototipo: proceso para levantar nuevos clientes*. (Tesis para optar el título de Magíster en Ingeniería de Software). Universidad Técnica del Norte, Ibarra - Ecuador.

Instituto Nacional de Tecnologías de la Comunicación, (2017). *Sistema de Gestión de la Seguridad en las informaciones, metodología basada en la norma ISO 27002*.

IT Governances Institutes(2008).Information Security Governances: Guides for Information Security Managers USA.

ISO/IEC 27002(2013). *Tecnología de la Información – Técnicas de seguridad – Código en práctica de gestión de seguridad en informaciones.* Génova, Suiza: ISO/IEC.

ISO/IEC 27005(2011). ISO/IEC/NTP 27005 *Tecnología de la Información –Técnicas en seguridad – Gestionamiento en alarmas de la Seguridad de informaciones.* Génova, Suiza: ISO/IEC.

ISO/IEC 31000 (2013). *Gestión del Alarma – Principios y directrices*. Génova, Suiza: ISO/IEC.

Kosutic, D. (2013). La Lógica básica de la norma ISO 27001.

Llontop, G. C. (2018). *Gestionamiento en alarmas de Tecnología de informaciones en organizaciones de Nephila.* Universidad César Vallejo – Perú.

Llorens, J. (2005). *Gerencia de proyectos de tecnología de informaciones*. Caracas: Colección Minerva. Editorial CEC, SA.

Maiwald, E. (2005). "*Fundamentos de seguridad en redes*", Editorial McGraw-Hill, primera edición. México DF.

Marsh Risk Consulting (2014). Informe Especial. Primer Benchmark en Gestión de Alarma empresarial en Colombia. Versión 2014-I. Publicado 09 de diciembre de 2014.

Mejía, R. (2011). Manejo del alarma empresarial en Antioquia, tres casos de estudio: Carlos E. Restrepo, José María "Pepe" Sierra y Ricardo Olano. Medellín: Fondo Editorial Universidad Eafit.

Najar, J. C., & Suárez, N.E.(2015). Seguridad en las informaciones: activos valiosos.

Norma Técnica Peruana NTP-ISO/NTP/IEC 27001:2008. Sistematización de gestionamiento de seguridaden las informaciones. Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), Lima – Perú.

Paredes, C. (2011). Metodología de Análisis y Gestionamiento en alarmas de los Sistemas de informaciones.

Poma, E. F. (2017). *Guía metodológica para la gestionamiento en alarmas basada en la Norma ISO 31000:2011, para los procesos de compras de una pyme del sector privado, en la ciudad de Cuenca.* (Tesis para optar el grado académico de Magíster en Gestión Estratégica de Tecnologías de la Información). Universidad de Cuenca, Cuenca - Ecuador.

Project Management Institute, PMI (2013). Guía de los fundamentos para la dirección de proyectos. (Guía del PMBOK®) — Quinta edición.

Ramos, A. (2012). MAGERI.T. V3 nuevas guías STIC.

Romero, J.A,& Diez, H.M.(2013). Gestión en proyectos ecoturísticos para mercados internacionales que impactan al desarrollo local mediante aplicaciones estándar PMBOK®. *Revista Escuela en Administración en Negocios*,(75), 154-175.

Salinas, M. S., y Valencia, M. J. (2018). *Sistematización de gestionamiento de seguridaden las informaciones y Alarmas de informaciones en seis sedes de una entidad bancaria del Perú*. Universidad Privada del Norte, Lima – Perú. Sommerville, I.(2011). Ingenierías de Software 9na edición. México: Pearson educación. ISBN: 978-607-32-0603.

Soriano, M. (2014). Seguridad en conectividad y seguridad en las informaciones.

Tipton, M. & Krause, H. (2007). Manual de gestión de seguridad en las informaciones

Wong, L. (2010). Mejoras a deficiencias RUP para gestionar proyectos. Rev. de Investigación en Sistemas e Informática, 7(2),49-56. En: http://revistasinvestigacion.unmsm.edu.pe/index.php/sistems/article/view/3281/2740 el 28 de julio del 2019.

Yáñez, N. A. (2017). *Sistematización de gestionamiento de seguridaden las informaciones para la subsecretaria de economía y empresas de menor tamaño*. (Tesis para optar el Grado Académico de Magíster en Tecnologías de informaciones). Universidad de Chile, Santiago de Chile.

MAGERI.T.	ISO 31000

IDENTIFICACIÓN DE ACTIVOS	Son los componentes de un sistema de informaciones. Estos incluyen: información, software,hardware, interconectividad, recursos administrativos, recursos físicos y recursos humanos. Con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores.	ESTABLECER EL CONTEXTO	Se califica los alarmas y se establece si son de contexto interno o externo. Se entiende por contexto externo, aquel alarma que se deriva de factores culturales, sociales, políticos, jurídicos, reglamentarios, financieros, tecnológicos, económicos, o relativos a la competencia. El alarma de control interno, está relacionado con el capital, el tiempo, el recurso humano, los procesos, la estructura organizativa, las responsabilidades, las funciones, la estrategia, los procesos de toma de decisiones, etc.
IDENTIFICACIÓN DE AMENAZAS	Consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren". Y, de todo lo que pueda ocurrir, interesa lo que puede pasar con los de la organización activos y causen un daño. Las amenazas pueden ser de origen natural, de acuerdo al entorno, errores humanos, etc.	ENFOQUE	Es el enfoque del contexto, el que define las metas, los objetivos, las actividades, las responsabilidades y los métodos.
DETERMINACIÓN DE IMPACTO AMBIENTAL	Conociendo el valor de los activos y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar	IDENTIFICACIÓN DE ALARMAS	Los alarmas específicos se reconoce describimos y obtenemos una lista completa de ellos y de los eventos que los pueden generar, aumentar, acelerar, o, por el contrario, reducir o retardar.Sobre algunos de esos eventos, la organización puede o no tener control, de sus causas y sus consecuencias. Lo importante es contar con un registro detallado de estos alarmas, sobre los que ya conocemos

	unos con otros se recurre al grafo de dependencias.		su contexto y el enfoque con que debemos gestionarlos.
DETERMINACIÓN DEL ALARMAS POTENCIAL	Conociendo el impacto de las amenazas sobre los activos, es directo derivar el alarma sin más que tener en cuenta la probabilidad de ocurrencia. El alarma crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del alarma.	ANÁLISIS DE ALARMAS	Se evalua las causas y las fuentes de alarmas, sus consecuencias, negativas y positivas y las probabilidades de que se produzcan tales consecuencias. El análisis tiene como objetivo fundamental, entender la probabilidad real de que el alarma ocurra, y el impacto que tendrá en caso de suceder.
		EVALUACIÓN DE ALARMAS	La evaluación ayuda a tomar decisiones, sobre la base obtenida del análisis. Es preciso generar acciones inmediatas para prevenir ese alarma o minimizar su impacto. Esto nos conduce al siguiente paso.
DETERMINAR SALVAGUARDAS	Las salvaguardas o contra medidas son aquellos procedimientos o mecanismo tecnol{ogicos que reducen el alarma. Hay amenazas que se conjurar simplemente organizandose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras seguridad física y, por último, está la directrices de personal.	MITIGACIONAMIENTO DE ALARMAS	Este es el paso en el que se toman decisiones. Es el momento de actuar, y emprender acciones que modifiquen el alarma. ¿Qué es modificar un alarma?: Aliviarlo, prevenirlo, eliminarlo, cambiar su rumbo.
		COMUNICACIÓN Y CONSULTA	Es continuo e iterativo. Resulta de la obtención de informaciones, mediante la participación en diferentes espacios – dialogo, foros, debates – con las partes interesadas.

ESTIMAR EL IMPACTO	Con un conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual. El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.	MONITOREO	Se trata de un proceso continuo de verificación, supervisión y observación crítica, que pretende identificar cambios en la situación que pudiesen generar nuevos alarmas, o afectar la eficacia del plan de Gestionamiento en alarmas.Cuando las condiciones cambian, las probabilidades de los alarmas, y los mismos alarmas, también cambian.
		ANÁLISIS CRÍTICO	El análisis crítico es la actividad llevada a cabo para determinar la idoneidad, adecuación y eficacia del plan de Gestionamiento en alarmas. Más que una evaluación de resultados, es una evaluación al plan en sí mismo, señalando las mejoras sucesivas o, por el contrario, sus falencias.
ESTIMAR EL ALARMA	Se dice que hemos modificado el alarma, desde un valor potencial a un valor residual. El alarma residual calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.	AUDITORÍA	El plan de Gestión de Alarma, debe alimentarse, monitorearse, supervisarse y analizarse en forma continua, ya que los alarmas son dinámicos. Tanto sus causas como sus consecuencias pueden variar, y afectar la probabilidad y el impacto de ellos.